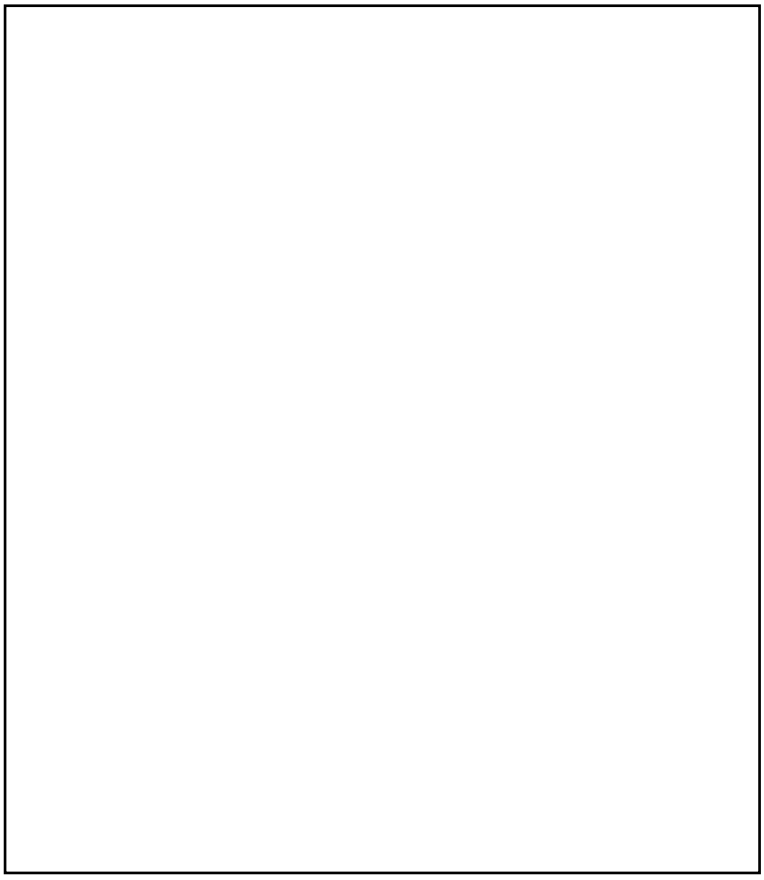
Ciberseguridad en Costa Rica

PROSIC
Programa Sociedad de la Información y el Conocimiento
Universidad de Costa Rica



PROSIC
Octubre 2010
Tel: 2253-6491 / Fax: 2234-5285
prosic@rectoria.ucr.ac.cr
San José, Costa Rica
Diagramación: Ana María Barboza Coto
Alfredo Alvarado Fonseca
Roberto Cruz Romero
Ilustración: Ana María Barboza Coto
Impreso por: Impresión Gráfica del Este S.A

Contenidos

Presentación

El desarrollo explosivo de las tecnologías de la información y la comunicación (TIC), referidas fundamentalmente a la informática (uso de las computadoras) y las telecomunicaciones (Internet) ha modificado radicalmente el quehacer humano y transformado los patrones de comportamiento y las relaciones sociales.

Los beneficios que las TIC aportan a la sociedad actual son diversos y evidentes. Sin embargo, el amplio desarrollo de estas tecnologías ofrece también un aspecto negativo: ha abierto la puerta a conductas antisociales y delictivas que se manifiestan de formas que hasta ahora no era posible imaginar. Han surgido nuevas maneras de atentar contra la privacidad y el patrimonio de las personas y las empresas, y para cometer delitos de tipo tradicional en formas no tradicionales.

Los llamados delitos informáticos, que constituyen actos delictivos que se cometen con la ayuda de las TIC y que aumentan los riesgos en el ciberespacio y ponen en entredicho la seguridad informática, se han ido multiplicando en los últimos años de manera exponencial.

Son numerosas las formas y los ámbitos en que se presentan los ciberdelitos. En términos generales se reconocen cuatro grandes

categorías: fraudes cometidos mediante la manipulación de computadoras, las falsificaciones informáticas, las modificaciones de programas o datos computarizados, y el acceso no autorizado a servicios y sistemas informáticos.

A manera de ilustración pueden citarse los siguientes delitos informáticos: violación de la privacidad, divulgación de material ilegal, sustracción de datos, modificación de los programas existentes o inserción de nuevos programas o rutinas (virus y gusanos), fraude bancario, espionaje informático e incluso ataques de naturaleza militar a las plataformas informáticas de un país (ciberguerra), etc.

Desde el punto de vista tecnológico, la aparición de aplicaciones cada vez más complejas y costosas para la protección de equipos y redes disminuye el riesgo, pero no garantiza inmunidad total. El sistema jurídico casi siempre va un paso atrás en cuanto a la creación de un marco normativo que permita sancionar a los hackers y a los piratas informáticos. Y la identificación y captura de las personas y organizaciones criminales que han hecho un negocio del robo de identidades, los fraudes virtuales y las agresiones infecciosas, conllevan dificultades inherentes y demandan especialización y gran cantidad de recursos represivos.

A estas dificultades debe agregarse el hecho de que los ciberdelitos son por lo general de naturaleza "global", es decir, ocurren en ámbitos que transcienden las competencias nacionales. Así lo reconoce el Programa de Acción de Túnez para la Sociedad de la Información en el que se destaca "la importancia de luchar contra el cibercrimen, incluido aquél cometido en una jurisdicción pero que repercute en otra." También se enfatiza "la necesidad de concebir instrumentos eficaces y mecanismos eficientes, a nivel nacional e internacional, para promover la cooperación internacional entre los organismos encargados de aplicar la ley en materia de ciberdelito."

Este conjunto de elementos y circunstancias ponen en evidencia que enfrentar las amenazas informáticas no es una tarea fácil. En verdad se requiere de una cultura de la ciberseguridad, cuyos rasgos principales deben incluir: la sensibilización sobre el problema,

la responsabilidad, la respuesta oportuna, el respeto a los intereses legítimos, la adhesión a los valores democráticos, la estimación de los riesgos, la implementación de los instrumentos de protección, la gestión de la seguridad, y la evaluación continua (Resolución 57/239 de la ONU).

En Costa Rica la seguridad informática, aunque aparece con bastante frecuencia en la cotidianidad de las personas y las organizaciones que enfrentan situaciones concretas de ataques informáticos, no ha sido abordada de manera integral ni ha constituido materia de atención explícita por parte de una población y de una institucionalidad que cada vez con mayor frecuencia e intensidad emplea las tecnologías de la información y la comunicación.

En general, la ciberseguridad se circunscribe a la esfera de los expertos y no se ha avanzado lo suficiente en el desarrollo de una cultura colectiva en este campo. Este libro pretende ser una contribución del Programa de la Sociedad de la Información y el Conocimiento de la Universidad de Costa Rica (PROSIC) a ese esfuerzo de creación cultural.

En la obra se incluyen las contribuciones de casi medio centenar de especialistas que desde diferentes perspectivas abordan el tema de la ciberseguridad. Muchos de esos aportes son ponencias (transcripciones hechas por Keilin Molina) presentadas en las Jornadas sobre Ciberseguridad organizadas por el PROSIC en el segundo semestre de 2009 y coordinadas por Marta Guzmán. Otros son artículos escritos para el libro. Agradecemos a todos los autores por su colaboración y confiamos en que tanto de manera individual como en su conjunto este trabajo sea de utilidad y provecho. También damos las gracias a las instituciones y empresas que contribuyeron a esta publicación: Fundación Paniamor, ITS InfoComunicación, Symantec, Fundevi y Managed Security Agency SA.

Juan Manuel Villasuso
Director PROSIC

Introducción

Uno de los objetivos del PROSIC es examinar el impacto que las nuevas tecnologías de la información y la comunicación tienen sobre las personas y la sociedad costarricense. Conscientes de la importancia que los delitos informáticos tienen en el quehacer diario, se consideró conveniente convocar a un grupo de personas conocedoras de la ciberseguridad para analizar sus distintas vertientes y examinar lo que se hace en Costa Rica en la actualidad.

Con ese propósito, el PROSIC organizó en la UCR, durante el segundo semestre del 2009 las Jornadas sobre Ciberseguridad. Se realizaron 16 mesas redondas en 8 sesiones de trabajo, en las cuales participaron cerca de medio centenar de expertos. Las ponencias se transcribieron y fueron complementadas con otros trabajos. El material se organizó en los diez capítulos que conforman este libro y cuyos rasgos más relevantes se detallan a continuación.

El Capítulo 1, *Conceptualización de la ciberseguridad* hace un repaso de la seguridad en el ciberespacio e incluye tres trabajos. La exposición de Luis Paulino Mora se refiere a los retos y oportunidades que se plantean frente a los permanentes cambios en materia tecnológica. Asegura que “los usuarios deben tomar conciencia de

que su vida y comportamiento están siendo estudiados para todo tipo de fines". Alfredo Chirino define los orígenes del concepto de ciberseguridad y sus dimensiones: política, económica, social y legal. También enumera los riesgos que conlleva la falta de regulación. Gabriela Barrantes expone sobre la importancia de definir los distintos tipos de amenazas, así como las vulnerabilidades y ataques asociados a la seguridad informática. Oldemar Rodríguez explica el Vector-Personal, un método matemático para detectar la atipicidad en el comportamiento de una máquina o una persona que permiten identificar los fraudes en tarjetas de crédito o débito, en las cuentas corrientes y en las transacciones bancarias.

El Capítulo 2, *Ciberseguridad y privacidad* plantea temas asociados con la identidad virtual y los datos personales. La ponencia de Marvin Carvajal versa sobre la seguridad de la información: confidencialidad, integridad y disponibilidad; y aclara como la autodeterminación informática es un derecho fundamental de toda persona para que su información sea procesada y manipulada de manera legítima. Federico Malavassi, por su parte, asegura que los datos públicos responden al derecho a la información, a la libertad de buscar, difundir y comunicar; en consecuencia, los datos gubernamentales no deben ser objeto de ningún control, pero sí deben responder a criterios de exactitud y veracidad. Francia Alfaro enfoca su trabajo en la privacidad de las redes sociales y las conductas en línea que implican un mayor riesgo en la filtración de los datos personales. Milena Grillo y Walter Esquivel, examinan los contenidos en línea asociados con la explotación sexual, la apología de la violencia, el racismo y la homofobia, así como las amenazas a la privacidad, especialmente en el caso de las niñez. También elaboran sobre las medidas de promoción de la seguridad y de prevención de los riesgos para los menores de edad.

El Capítulo 3, *Firma digital y ciberseguridad* refiere a un aspecto concreto de la evolución hacia la Sociedad de la Información. Carlos Melegatti define la manera como en el mundo digital, la configuración de las claves de acceso a los múltiples sistemas informáticos son complejas de administrar y proteger, razón por la que se ha

implementado la firma digital certificada, orientada a brindar al ciudadano facilidad y seguridad a la hora de hacer las transacciones. Luis Roberto Cordero, hace un análisis entre la ciberseguridad y la firma digital; afirma que "la ciberseguridad trata de la seguridad y la disponibilidad de la información, y que a la firma digital compete a la vinculación jurídica de la información con su autor. Pero no olvidemos dice, que el eslabón más débil sigue siendo el usuario final". Oscar Solís explica como el Sistema Nacional de Certificación Digital implementa mecanismos robustos contra la suplantación de la identidad, robo de información y fraude. Además, examina los mecanismos de autentificación y firma para los usuarios.

El Capítulo 4, *Tipo y naturaleza de los ciberdelitos* tiene un enfoque esencialmente jurídico tanto de orden conceptual como sustentado en el derecho positivo. Christian Hess hace un recuento de la tipología de los delitos informáticos, la dificultad de identificarlos para su persecución y las soluciones y tendencias legislativas. Carlos Chinchilla detalla el vínculo de los ciberdelitos con el derecho penal económico en Costa Rica y explora los tipos penales informáticos y la legislación que se aplica en el país. José Francisco Salas se enfoca en algunos de los errores y omisiones de la legislación costarricense en el campo de los delitos informáticos; asimismo, hace una amplia explicación del convenio de Europa sobre la ciberdelincuencia.

El Capítulo 5, *Prevención y sanción de los ciberdelitos* permite profundizar en aspectos concretos del marco normativo de la ciberdelincuencia. Erik Lewis, analiza como la mayoría de los fraudes informáticos se basa en la ingeniería social: ciencia de manipular a las personas para obtener información confidencial. También precisa los diferentes modos de operar de los delincuentes y su evolución en el tiempo. Adriana Rojas advierte de las modalidades que usan los delincuentes para atacar a los sistemas informáticos y sus usuarios; además, hace referencia a algunos casos de delitos en línea. Georgina García reseña algunos de los delitos que afectan los derechos de propiedad intelectual en el mundo informático. También hace un recuento de desarrollos legislativos recientes y los problemas de aplicación, así como los retos en el entorno digital.

El capítulo 6, *Las TIC y la seguridad nacional*, aborda dos ámbitos de gran importancia, el de los desastres naturales y el de los actos ilícitos que se cometen utilizando las tecnologías digitales y que ponen en riesgo la integridad del Estado. Mauricio Mora describe el papel de las TIC en la prevención de los desastres naturales, para lo cual se construyen complejas estructuras de bases de datos y sistemas de información geográfica. Sergio Sánchez explica la forma como la Comisión Nacional de Emergencias utiliza las nuevas tecnologías en la prevención de los desastres naturales en Costa Rica y detalla el tipo de amenazas hidrometeorológicas y geológicas, así como la importancia de la información geoespacial en la toma de decisiones. Celso Gamboa, por su parte, aborda el tema del ciberterrorismo. Comenta sobre los factores que convirtieron la seguridad cibernética en una necesidad mundial y como ese peligro llevó a la creación en Costa Rica de un *"equipo de respuesta ante incidentes de seguridad cibernética"* (CSIRT) cuyo objetivo principal es contribuir con la seguridad y defensa del espacio nacional (soberanía cibernética).

El capítulo 7, *Protección de redes*, tiene un enfoque más tecnológico. Jorge Blanco pormenoriza sobre el tipo de ataques que aprovechan las vulnerabilidades de los sistemas para entrar en la infraestructura de las redes de las empresas e instituciones. Además, pone en discusión la responsabilidad que tienen los administradores de las redes. Richard Elizondo establece la diferencia entre la seguridad informática y la seguridad de la información. Asegura que el resguardo de la información es lo realmente relevante pues si esta se pierde todos los elementos de la red dejan de tener importancia. Jonathan Solano hace un recuento de los distintos tipos de amenazas que sufren las empresas en sus redes y sus sistemas de información. Enfatiza que las organizaciones "deben estar claras de cuánto vale la información en sus bases de datos, para así definir qué es confidencial, qué compartir y qué niveles de acceso proporcionar". Advierte sobre la necesidad de disponer de un sistema de gestión de la seguridad informática (SGSI) que contemple todos los ámbitos logísticos y físicos de los sistemas. Jairo Villalobos señala las soluciones para prevenir las estafas y los fraudes en los bancos y ofrece

una serie de ejemplos de las técnicas más usadas por los *hackers* para vulnerar los sistemas financieros.

El Capítulo 8, *Protección de equipos*, es complementario del anterior y también tiene un enfoque tecnológico. Luis Diego Espinoza destaca la importancia de tomar en cuenta la parte física y social de las amenazas cibernéticas. Señala que "la tecnología ayuda, pero es costosa y compleja y no constituye la solución definitiva para protegerse de los ataques, hay que crear conciencia y educar a los usuarios". Edgardo Baltodano describe de manera detallada los tipos de virus, *spam*, troyanos, gusanos, *hoaxes, phising, rookit y spyware,* así como la forma en que afectan los equipos y lo que debe hacerse para evitarlos. Luis Diego Esquivel se enfoca en la responsabilidad al utilizar las tecnologías, la importancia de tener las reglas claras para la familia y, sobre todo, para los niños que son los más vulnerables. También comenta sobre las principales amenazas en línea, el robo de identidad, la invasión a la privacidad y las formas de proteger la computadora y los equipos en general. Miguel Garro analiza los retos y responsabilidades que tienen los gerentes de la seguridad de la información de las empresas. Señala que la protección de datos debe enfocarse en una correcta administración de los riesgos y respuestas rápidas y eficientes ante los incidentes.

El capítulo 9, *Protección de datos* articula los dos capítulos anteriores desde la perspectiva de los expertos en seguridad informática. Jorge Castro se refiere a la importancia de normar la seguridad que tienen los repositorios de información de las empresas que se dedican a consolidar datos. Asegura que "no hay una sola política o ley que le exija a estas compañías los controles mínimos para el manejo de la información". Álvaro Jaikel enfoca su ponencia en los principales retos que enfrentan las organizaciones en seguridad de la información y manifiesta que estos deben ser atendidos con una visión más preventiva que curativa. También comenta sobre la labor de la Asociación Costarricense de Auditores en Informática, reconocida como Information Systems Audit & Control Association (ISACA). Jessica Calvo explica la manera en que Internet, basado en el *Sistema de Nombre Dominio*, hace una diferencia

entre dominios genéricos *(.com, .net y .org)* y los dominios código país. Además, explica que la Academia Nacional de Ciencias, por medio de la unidad NIC-Internet, es la que se encarga en Costa Rica de la operación del *Dominio Superior .cr* y establece las políticas y protocolos.

Nicolás Severino revela como la ciberdelincuencia ha dado origen a una economía clandestina en Internet y explica la manera como se comercializan datos y la información de personas y empresas. Además, presenta estadísticas que muestran la evolución de los delitos informáticos en el ámbito internacional. Por su parte Luis Cerdas asegura que toda información debe ser protegida para cumplir con al menos un mínimo de seguridad en su manejo y gestión. La única forma de tomar control de la información, es por medio de la seguridad administrada de la información. Este es un proceso que incluye la identificación y la categorización de la información, la definición de políticas empresariales sobre el manejo de la información; el alineamiento de estas políticas con la estrategia empresarial; y finalmente, el ciclo de implementación, valoración y mejoramiento.

El capítulo 10, *Casos de seguridad informática,* recoge las experiencias en materia de seguridad informática de varias instituciones y empresas relevantes en Costa Rica: Gobierno Digital, Caja Costarricense del Seguro Social, Banco Nacional, Poder Judicial, Registro Nacional, Tribunal Supremo de Elecciones y Contraloría General de la República. Cada una de estas instituciones hace referencia a los estándares de seguridad informáticas aplicadas, las políticas establecidas, los desafíos que han tenido que enfrentar y las soluciones que han desarrollado.

La lectura de estas contribuciones lleva a la conclusión de que es necesario inculcar una cultura de ciberseguridad, a la manera de las prácticas de salud preventiva o de la seguridad vial. La cultura de ciberseguridad es transversal pues alcanza a individuos, empresas, instituciones y, en general al país.

Marta Guzmán

Coordindora

Capítulo 1
Conceptualización de la ciberseguridad

Para ser víctima, basta estar conectado

Luis Paulino Mora Mora

Esta publicación de análisis sobre los "Delitos Informáticos y la Ciberseguridad" se produce sin duda en un momento en que el mundo vive, más que nunca, dramáticos cambios en materia de tecnología que impactan drásticamente todos los aspectos de las relaciones humanas. Esto nos presenta como una sociedad de enormes oportunidades, pero también de grandes retos.

La nueva era tecnológica muestra un mundo virtual absolutamente interdependiente con el mundo real, del cual dependemos cada vez más. El ciberespacio es real y reales son también los riesgos que vienen con él. Dependemos de la Internet cada vez más, para hacer nuestras transacciones bancarias, pagar recibos, hacer compras, trabajar y gozar de ratos de ocio y eso es aprovechado por algunos para sacar ventajas ilegítimas. Unos para espiar, otros para robar. Así surge el *spoofing, phishing* y otros términos nuevos a los que los ciudadanos apenas nos acostumbramos. Dineros robados, identidades robadas, violación a la privacidad, espionaje corporativo, son sólo algunos de los retos que nos presenta esta nueva era de la interconectividad.

Sólo en los Estados Unidos de América en los últimos dos años, se estima que el cyber crimen ha costado más de 8 billones de dólares a los americanos. La propia seguridad informática del actual Presidente Obama fue violada durante su campaña presidencial. Por otra parte, las cifras sobre el cyber crimen y las pérdidas en propiedad intelectual a nivel mundial se estiman en un trillón de dólares. El propio Presidente de los Estados Unidos ha señalado que la prosperidad de su nación en este siglo dependerá sustancialmente de la Ciberseguridad.

Las potencias mundiales sufren este fenómeno no sólo como pérdidas individuales o empresariales, sino también como un tema de seguridad nacional. Dependen de la interconectividad para mover el transporte público aéreo y terrestre, transar y transportar el petróleo y gas, interconectar el ejército, conectar la electricidad, mover y transar capitales, en fin, para todo. Tanto dependen los países desarrollados de sus redes de computación y la interconectividad, que se estima que el próximo ataque terrorista será un cyber ataque, capaz de paralizar la economía norteamericana.

En un tono más local, puedo decirles que en nuestro país el cyber crimen crece cada vez más. Puedo dar fe de ello, porque mi familia se encuentra entre las víctimas del *phishing*, de tal forma que esta realidad no discrimina y está presente en economías grandes o pequeñas. Para ser víctima, basta estar conectado.

Esta nueva realidad también nos revive permanentemente la pesadilla de Orwell. La amenaza Orwelliana cobra una inevitable realidad frente a la era tecnológica, sólo que la amenaza no está sólo en el Estado, sino frente a la cibercriminalidad en general, que se puede apropiar de nuestros datos, para venderlos o controlar directa o indirectamente nuestras vidas. A manera de ejemplo hay cientos de redes de cámaras que pueden ser *hackeadas* o información de *cookies* que puede ser cruzada para construir nuestro perfil de consumidor e invadir nuestra privacidad.

A través de los *cookies* como ustedes saben bien, se puede recoger y almacenar cuáles páginas visitó un internauta, cuánto tiempo pasó

en cada una de ellas, qué *software* usó durante el proceso, si tuvo dificultades para navegar, su grado de idoneidad en el manejo de la red, etc. Con esa información, *cookie* comenzará a armar un detallado mapa personal: sus gustos, sus hábitos, su perfil consumidor, su potencial como cliente, sus conocimientos, sus debilidades, etc. En síntesis, la herramienta de marketing personal perfecta y un gran negocio para los creadores y proveedores de *cookies*, una tecnología muy usada por los *sites* en forma directa o a través del *software* de los anunciantes que adquieren sus banners.

La información obtenida por *cookie* -sin consentimiento ni conocimiento del navegante- puede ser ampliada y de hecho lo es. Cada vez que se llena un formulario para suscribirse a una publicación *electrónica* o para hacer una compra *on-line*, la información se amplía y el sistema acopla los datos personales -nombre, dirección, teléfono, e-mail, número de tarjeta de crédito, etc.- al perfil anónimo archivado bajo un número. A partir de allí, la información deja de corresponder a un anónimo código de identidad y un simple cruce de datos (por ejemplo, la verificación del crédito disponible en su tarjeta) aporta información sobre la persona que crece en forma geométrica. De "XXNN" pasa a ser "Fulanito de Tal", 38 años, administrativo de un laboratorio de especialidades veterinarias, 3 tarjetas con un crédito aceptable, cliente de 2 bancos con un buen registro de cumplimiento de obligaciones, vive en un barrio de buen perfil, le falta menos de 1 año para terminar de pagar el préstamo hipotecario, no tiene hijos, ni seguro de vida pero sí tiene miedo de quedarse sin su cabello, porque en el último año visitó 16 veces páginas en las que se habla sobre la recuperación del cabello. Además le gustan las carreras de autos y este fin de semana pasó 1 hora 23 minutos 48 segundos recorriendo los *links* de pornografía *hardcore* holandesa.

Sin duda alguna, existen ojos ocultos y omnipresentes que nos vigilan desde el espacio cibernético. Hace rato que sabemos que nuestros datos están en manos de terceros, pero estos temas están poco regulados y controlados.

Debemos enfrentarnos a la triste realidad de que nuestras huellas electrónicas pueden ser (y son) seguidas por sabuesos cibernéticos

para detectar nuestras debilidades. Por lo tanto, el tema de la invasión de la privacidad y manipulación de los datos personales en la red requiere la urgente atención de todos los sectores. Los usuarios deben tomar conciencia de que su vida y comportamiento están siendo estudiados para todo tipo de fines. Los dueños de los recursos invasivos deben entender que los límites son tan necesarios, como la información, y que el avasallamiento de los derechos de los usuarios puede terminar por volverse en su contra.

Por eso me parece muy importante enfatizar en una publicación como la presente, - en la necesidad como democracia que somos- , en la obligación de garantizar el respeto a la seguridad e intimidad de los ciudadanos, valores que debemos sopesar siempre a la hora de desarrollar cualquier estrategia de lucha contra la criminalidad en cualquiera de sus formas.

Tanto la legislación como la administración de justicia, tienen por lo tanto, que estar a la altura de estas nuevas formas de criminalidad. Pero son foros como el presente los que nos ayudan a reflexionar y proponer soluciones reales a problemas actuales. Mis felicitaciones a PROSIC y a la Universidad de Costa Rica por estar, una vez más, a la altura de los retos actuales y garantizar que la búsqueda de soluciones frente a los retos de la nueva era tecnológica, se harán siempre dentro de la vigencia de los valores democráticos.

Hacia un concepto de "ciberseguridad"

Alfredo Chirino Sánchez

El ciberespacio ¿Existe?

Este concepto surge de la mano de la ciencia ficción. Fue William Gibson en su novela "Mona Lisa Acelerada" quien plantea por primera vez la idea de un "ciberespacio". Este mismo autor, tiempo antes de este libro, había introducido la sugerencia de un mundo que puede existir más allá de lo físico, más allá de lo material, en suma, un ambiente artificial donde el erotismo, la relación entre lo físico y lo mecánico, lo real o lo irreal es plenamente intercambiable. Esta idea sería explotada de manera prodigiosa en la película de los hermanos Wachowski, "Matrix", donde lo inmanente y lo racional, lo real y lo soñado, la vida creída y la realizada cruzan sus fuerzas. La idea del "ciberespacio" vive de estas relaciones y entrecruzamientos, de esta puesta en escena filosófica entre realidad y ficción, entre vida material y vida onírica, entre lo perceptible por los sentidos y lo vivido más allá de ellos, en suma se trata de un campo donde el ser humano puede construir un mundo donde realiza lo que desee, se proyecta de la manera que le plazca y obtiene aquello que el mundo físico le niega o le condena a no tener.

La idea del ciberespacio se gesta en las galerías de videojuegos, en las conexiones neuronales y en la interconexión con el poderoso mundo electrónico, donde cantidades ingentes de información pueden sustituir nuestras sensaciones, conocimientos y experiencias. Esta idea primigenia del ciberespacio une lo lúdico con lo militar, lo vivencial con lo tecnológico y expresa un poder enorme, que empequeñece lo que hemos alcanzado con Internet, pero que al mismo tiempo potencia lo que hemos podido vislumbrar a través de una existencia interconectada y sin refugio para la soledad.

La antigua cibernética, la ciencia que intentaba explicar el movimiento, se confabula con esta idea compleja del "ciberespacio" y ya no es más que una parte de ese mundo interconectado al que conocemos como ciberespacio.

El ciberespacio parece que ya no es una realidad "post-punk" o el engendro de la imaginación inagotable de un escritor de ciencia ficción, sino que es una fábula que estamos escribiendo con una cultura dependiente de la tecnología, una red de experiencias que se extiende a todo el mundo, que todo lo toca y lo transforma. No podemos entender nuestra existencia actual sin el ciberespacio.

Los jóvenes de hoy en día construyen su mundo con estos contactos virtuales, con esta vivencia en red donde solo lo tecnológicamente compartido, sea por conexión vía chat o por correo electrónico o por mensajes SMS, realmente existe. Una invitación, una noticia o una información solo son válidas si viajan por ese medio. Ellos han demostrado que un mundo puede existir a través del prisma de estas interconexiones, y su vida solo se explica a través de dichos contactos. No formar parte de este mundo implica exclusión y hostilidad.

Las pautas de esta sociedad interconectada, que construye un ciberespacio a partir de conexiones de banda ancha a Internet, ya es, por sí misma, un interesante fenómeno de estudio. No sólo por las nuevas vivencias que nos condenan a estar siempre disponibles y presentes, sino porque toda nuestra comunicación depende de esta interconectividad. El teléfono y no el computador se ha convertido en el centro de este desarrollo impresionante, no sólo por la confluencia de tecnologías que permite, sino por regentar allí incluso donde la

sociedad de mercado ha excluido al consumidor. El teléfono es hoy el centro neurálgico de la información que transita por las infovías costarricenses y del mundo y postula nuevas formas de etiqueta y de interrelación social. Olvidar el teléfono es quedar condenados a la exclusión, a no recibir noticias, en suma, a exponernos a no formar parte de los engranajes sociales. Tal dependencia era desconocida con las tecnologías previamente conocidas, quizá solo la televisión tendría esa cuota de fidelidad y dependencia.

Un ámbito abierto al riesgo

En este ambiente informativo, con intensidades directamente proporcionales al grado de penetración tecnológica que haya tenido el país, tenemos a un ser humano indefenso. No se trata sólo de ser objeto de observaciones no deseadas de nuestro intercambio epistolar o de nuestros contactos, apetencias y pecados, sino también por la posibilidad de ser víctimas de nuevas formas de delito y de violencia.

Nuestra generación ha visto cambios descomunales en las costumbres comunicativas, pero sin duda serán las generaciones futuras las que tendrán una cuota mayor de asombro. Ya viven nuestros jóvenes inmersos en comunidades virtuales donde se intercambian todo tipo de datos e informaciones, se invitan y se alejan, se conocen y se expresan. Estas nuevas formas de comunicación, la exhibición tan evidente de ámbitos de intimidad que nuestras generaciones cuidaban tan celosamente, son el ámbito en el que ahora debemos poner a prueba nuestros esquemas de valores.

Hasta ahora hemos dado una mirada a lo que tenemos a nuestro alrededor, con lo que convivimos y que apenas estamos empezando a comprender en toda su dimensión, sin embargo, el ciberespacio también se ha convertido en un objeto de regulación y de estudio científico. Recientemente los Estados Unidos, en su "Cyber Space Policy Review"[1] , con razón explican que el ciberespacio, prácticamente, toca a todos los seres humanos y a todo lo que los rodea. Se trata no sólo de una plataforma para la innovación y la prosperidad,

1 http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

según este documento, sino que también promete convertirse en un instrumento útil para alcanzar el bienestar para todo el mundo. Sin duda, se observa al ciberespacio de una manera totalmente positiva pero sin ocultar los riesgos que podría provocar dejar este tema sin regulación, vacío que podría provocar riesgos y peligros para las naciones, las empresas y los derechos individuales de los ciudadanos.

Es evidente que las infovías que han sido construidas a partir del acceso a Internet ofrecen diversos problemas de seguridad, donde sin duda el más importante es su crecimiento exponencial y sin control, donde nuevos sitios y ofertas de servicios, crecen por doquier en cualquier momento. Según estimaciones de la EMC Corporation, la información disponible en el mundo se habrá multiplicado por 45 para el año 2020. Lo producido en el 2009, año de crisis y recesión, se estimó en 0,8 zettabytes, es decir 800.000 millones de gigabytes, un aumento del 62% sobre lo producido en el año 2008[2], lo que obliga a pensar que en tiempos de bonanza y tranquilidad económica habrá sin duda un aumento importante en los porcentajes de información disponible y guardada en diversos repositorios digitales a lo largo del mundo, ofreciendo diversos problemas a los encargados de TIC en todo el orbe. Junto a ello habría que apuntar la posibilidad de que esta ingente cantidad de información oculte como una aguja en un pajar los riesgos para la seguridad mundial, tanto en términos de planes criminales para obtener beneficios indebidos del tráfago de información, como también para ocultar atentados y amenazas terroristas que pondrían en peligro la base de sustentación del ciberespacio y la sociedad que depende de él.

La Cyberpolicy de los Estados Unidos entonces apunta a un importante aspecto de la vida moderna: mantener la confianza en las infovías y en la infraestructura que las hace posibles, de tal manera que siga sosteniendo el desarrollo económico y social de los países, con garantía de que la delincuencia y el abuso de información estén bajo control. No hay duda que el impacto de las intrusiones informáticas y el robo de valiosos datos económicos e industriales

2 Cfr. "El ritmo de crecimiento anual de la información se habrá multiplicado por 45 en 2020", http://cibersur.com/internet/004817/informacion.

no solo provoca un efecto negativo en los ciudadanos, sino que también puede afectar la capacidad de reacción de los países frente a los riesgos tecnológicos.

La falta de atención legislativa a estos riesgos y la escasa capacidad para atender estas circunstancias tecnológicas, sin duda ofrece diversos inconvenientes. Por una parte no hay mucha sensibilidad social hacia los problemas que se presentan con las TIC sino que también se tiende a minimizar su papel en ámbitos tan sensibles como el de la intimidad y el patrimonio. Los instrumentos legales, no obstante, están a disposición del legislador y una reforma integral de la justicia penal se viene gestando desde inicios de la década de los años noventa, solo hace falta terminar de redondear los grandes avances que quedaron dibujados en los trabajos legislativos iniciados con el Proyecto de Código Penal de 1995, redactado por el profesor y catedrático universitario, de grata memoria, don Henry Issa El Khoury Jacob.

La amenaza del "cybercrime"

Los delitos informáticos gozan de una excelente coyuntura. No sólo se ha abaratado el acceso a más poder informático, ahora disponible en receptáculos cada vez más veloces y miniaturizados, sino que la memoria disponible para acarrear ingentes cantidades de datos se hace centuplicado desde los años noventa. Hoy un terabyte de capacidad de memoria en un computador es sumamente barato y se anuncia el aumento de esta capacidad en el próximo quinquenio. Con ello se ha alcanzado que la capacidad de computación iguale y supere la que ofrecen las instituciones estatales sino que también se haga móvil y fácilmente ocultable.

El software ha tenido un mejoramiento ostensible y cada día se optimizan también las capacidades creativas para promover nuevas formas de acceso ilícito a redes cerradas y abiertas, ambientes WIFI y WIMAX y la seguridad de las comunicaciones vive uno de sus tiempos más complicados. Al mismo tiempo que mejora el acceso de los ciudadanos a la banda ancha de Internet, en la misma proporción aumenta la capacidad de los delincuentes informáticos para

poner en peligro no sólo el reducto de intimidad del ciudadano sino también sus interacciones con otros ciudadanos, con las empresas en las que confía y con el Estado.

La estructura legislativa que intentaba generar alguna protección frente a estos peligros del desarrollo informático había sido construida a partir de los delitos tradicionales. El robo, el hurto, el delito de daños, la estafa y la divulgación de secretos se convirtieron en la base para crear descripciones de delitos informáticos, donde solo variaba el método de comisión. Este acercamiento bien pronto se demostró como inútil no sólo por la variedad de afectaciones que empezaron a detectarse, como por las dificultades para acercar esos delitos tradicionales a los nuevos medios de comisión de los ilícitos.

Bienes jurídicos tradicionales como la intimidad, la propiedad, el patrimonio y la seguridad, entre otros, empezaron a sufrir menoscabos extremos de manos de delincuentes informáticos, y aquella base tradicional de acercamiento legislativo se manifestó incapaz de contener estos avances. A ello hay que sumar las dificultades de investigación. En concreto, el seguimiento de delitos que por su propia conformación y organización son globales, organizados y altamente complejos se ha convertido en una de las mayores dificultades para la atención legislativa de las necesidades de la investigación. Al respecto los países claman por mayor cooperación internacional y en acciones que involucren autoridades penales de los diversos continentes.

Junto a los delitos tradicionales, surge hoy la preocupación por el así denominado "ciberterrorismo" que no es más que el uso tecnológico para crear terror y confusión. Este tipo de acciones, tales como impedir las comunicaciones, ralentizar la reacción de los Estados y crear confusión por la caída de la infraestructura informativa, son cada vez más probables. Amenazas de este tipo se han advertido luego de los sucesos del 9 de setiembre de 2001 y las condiciones para una adecuada reacción frente a ellas siguen siendo frágiles y cuestionables. Esto último, sobre todo, por la facilidad con que se puede afectar la delicada infraestructura de información militar, también porque las infovías han permitido el acceso y distribución de información

clasificada sobre secretos militares, riesgos que en conjunto pueden socavar la confianza del público en la capacidad estatal para reaccionar frente a este tipo de ataques terroristas.

A pesar del peso de estos peligros, la reacción estatal no puede dejar de tomar en cuenta que esa confianza pública también depende de la intensidad de la protección de los derechos fundamentales. Ese delicado equilibrio sigue siendo uno de los retos más trascendentales en el desarrollo de una política estatal de atención a estas amenazas.

Cyber space policy review

La Cyber Space Policy es un esfuerzo de los Estados Unidos por reducir la vulnerabilidad de su infraestructura informativa, pero también una oportunidad para trabajar en la prevención, generar cooperación internacional, así como para brindar seguridad y confiabilidad. Una política de seguridad en el ciberespacio que pueda ser implementada a nivel global podría dar las bases para una política de persecución de los delitos globales que hoy aquejan el mundo cibernético.

Estos delitos tienen la ventaja de contar con ministerios públicos y policías escasamente informadas y preparadas para investigarlos, con capacidad informática instalada deficiente, mecanismos legales obsoletos o pensados para otros horizontes de proyección, y con medios y herramientas cada vez más sofisticados en manos de los criminales, que ponen en entredicho la propia lógica de la investigación penal.

Hace poco, en una conferencia nacional, un investigador del Organismo de Investigación Judicial nos relataba la enorme incidencia que estaban notando de programas que viajan de manera oculta en inocentes mensajes de correo. La estrategia es sencilla y eficiente: la víctima recibe un correo de felicitación de cumpleaños o el mensaje de haber obtenido un premio, se le invita a hacer “click” en un link que contiene el mensaje o la confirmación del premio. La víctima, sin advertir el peligro, sigue el link sugerido y una vez allí provoca que un programa se infiltre en su computador y empiece a enviar información privada por medio de correos electrónicos a un criminal que se encuentra lejos de su hogar. Con los datos así obtenidos, muchas veces de su vida privada, cuentas de banco y de tarjetas de crédito,

los delincuentes atacan sus activos financieros, provocándole pérdidas económicas importantísimas. La estimación policial de los daños a patrimonios ronda los cientos de millones de colones.

El anterior panorama no sólo refleja la refinación y sofisticación de los medios disponibles para afectar a los ciudadanos, sino que también es ejemplo de nuestra escasa sensibilidad y educación para prevenir que estos y otros delitos puedan tener lugar.

Este es un tema interesante de investigación que no tiene que ver exactamente con la tecnología sino con la confianza que tenemos en las herramientas que nosotros mismos utilizamos, en el enorme océano de riesgo que existe.

Ciberseguridad y contrato social

En otro texto que se llama "Recomendaciones políticas para el contrato Social de ciber seguridad para la Administración Obama y el Congreso No. 111"[3] se plantea la cuestión que nos interesa en términos de un contrato social, pero esta vez firmado entre la industria y el gobierno federal para promover intereses comunes, y promover un mayor bienestar para los ciudadanos. Tal parece que el acercamiento político del gobierno de Obama pretende la generación de condiciones propicias para el desarrollo humano sin limitar las capacidades de la industria para generar riqueza.

Esto es esperanzador si se convierte en una política global. No hay que dejar de tomar en cuenta que las desigualdades globales en ingreso se han incrementado. Solo en el siglo XX estas desigualdades ya no tienen parangón con ninguna época anterior de la historia de la humanidad. El Reporte sobre Desarrollo Humano del año 2000, del Programa para el Desarrollo de las Naciones Unidas, indica que la distancia entre ingresos entre los países más ricos y más pobres era de cerca de tres a uno en 1820, de 35 a 1 en 1950, de 44 a 1 en 1973 y de 72 a 1 en el año 1992. Junto a ello, no sólo el ingreso

3 Cfr. Review and the Cyber Security Social Contract: Recommendations for the Obama Administration, publicada por la Internet Security Alliance en November 2008, disponible en: http://www.isalliance.org/images/stories/The_Cyber_Security_Social_Contract_122008.pdf.

se separa violentamente entre los países más desarrollados y los menos desarrollados, sino también el acceso a la tecnología y a las ventajas del acceso a la información.

El acercamiento del Gobierno Obama tiene, sin duda, una oportunidad estratégica que apunta en la dirección correcta[4].

Sentido económico del contrato

Bien, el contrato social tiene un sentido económico, ¿para qué? Para que las autoridades se garanticen que los inversiones en el sector telecomunicaciones, tecnología, también lleguen a nosotros. ¿Cómo retornan? A través de la inversión privada.

Según el documento bajo análisis, la estrategia norteamericana había sido construida para motivar el desarrollo incipiente de los ferrocarriles en dicho país del Norte. A pesar de los cambios tecnológicos, el problema y el desarrollo de los ferrocarriles se mantiene similar, no así la Internet, un ámbito donde los desarrollos son intensos y cambian de manera violenta en poco tiempo. El brindar seguridad a un campo tan cambiante no sólo consume mucho tiempo sino que hace que toda política que nace pronto se convierte en obsoleta por los cambios ingentes que se producen, a veces en el transcurso de un solo día[5].

Junto a lo anterior, el documento puntualiza los riesgos de políticas de transparencia democráticas al tomar estas decisiones legislativas, que involucran, muchas veces, la publicación de textos de gran sensibilidad para la seguridad interior de ese país. Compara los esfuerzos hechos para cambiar el sistema de financiamiento de los partidos políticos con el escaso éxito obtenido en impactar los temas que realmente interesaban con una normativa que terminó siendo minimalista[6].

4 Cfr.http://information-security-resources.com/wp-content/uploads/2009/12/social-contract-20-final-implementing-the-obama-cyber-security-strategy1.pdf.
5 Cfr. Implementing the Obama Cyber Security Strategy via the ISA Social Contract Model, op. cit., p. 2.
6 Ibid., p. 3.

El contrato social en material de ciberseguridad, como el propio documento lo refiere, contiene dos certezas que son importantes, por una parte que el tema de la ciberseguridad no es sólo un problema técnico sino que es mucho más un tema que involucra a las empresas desde la perspectiva de sus políticas de manejo de riesgos. Estas políticas deben ser analizadas, según el documento, a partir de un análisis económico de sus consecuencias. Por otro lado, y esto es trascendente, se define que el rol más importante del gobierno es motivar e impulsar la inversión requerida para implementar los estándares, las prácticas y las tecnologías que han demostrado mejores éxitos en materia de ciberseguridad. Pragmáticamente se sugiere que el propio mercado privado ha hecho estudios y ha diseñado tecnologías que han demostrado éxito ante las constantes amenazas y ataques que suceden en Internet, y esta experiencia acumulada y generada a partir del interés sectorial de las empresas de información, podría generar una masa crítica de conocimiento que podría provocar un estándar exitoso de seguridad. Tan solo falta, lo sugiere el documento, la voluntad de aplicar dichos estándares al problema, en suma, el tema es: implementación[7].

El propio documento bajo análisis refiere a la encuesta denominada "The Global Information Security Survey, que fue conducida por Pricewaterhouse Coopers[8]. Este estudio reveló que las empresas que siguieron las mejores prácticas tuvieron cero impactos en su trabajo y en sus finanzas a pesar de haber sido escogidas como objetivos de los delincuentes en la red. Conclusiones similares arrojó el estudio conducido por Verizon, titulado: "2008 Data Breach Investigations Report"[9]. Este reporte concluyó que en el 87% de los casos se hubiera podido evitar la infiltración en sistemas de información si tan solo se hubiera contado con razonables controles de seguridad para el momento de los incidentes.

7 Implementing the Obama Cyber Security Strategy via the ISA Social Contract Model, op. cit., p. 4.
8 Is Cyber Security Improving in the Business World, Why? or Why Not?, Presentation by John Hunt, Principle PricewaterhouseCoopers, on the results of the 2009 Global Information Security Survey, University of Maryland, October 28, 2009.
9 Verizon Business Risk Team, 2008 Data Breach Investigations Report at 2-3, disponible en: http://www.verizonbusiness.com/resources/security/databreachreport.pdf.

Si se hace caso a las conclusiones de estos trabajos podríamos coincidir no sólo en que los ataques informáticos pueden ser evitados sino que también bastaría con un poco de esfuerzo de implementación y en crear una cultura de control y seguridad en el ámbito público y privado.

¿Economía de la ciberseguridad?

En los términos en que está planteado el argumento del impacto económico es fácilmente entendible la mirada estratégica que está haciendo el gobierno del Presidente Obama, trasladando buena parte del factor clave a la estructura productiva de su país, la que, además está atenta a estos fenómenos con una sensibilidad especial propiciada por los riesgos que afrontan en el mundo de hoy.

El ciudadano común, el que todos los días se debate entre la protección de su intimidad y el uso cada vez más intensivo de las tecnologías, tiene ante sí un camino minado. Sus correos pueden ser desviados, observados o copiados. Recibe cantidades inmensas de SPAM. La información que consulta en la Internet deja un rastro que puede ser fácilmente seguido por aquellos que tengan interés en perfilarlo como un potencial cliente o una potencial víctima. Y además de todo eso, está expuesto a ser víctima de investigaciones policiales en curso que observan, de manera secreta, las interconexiones sospechosas, y sin saberlo se convierte en parte de toda una trama detectivesca, hasta que el propio proceso automático que lo tomó como sospechoso lo descarta como tal.

Toda esta exposición al peligro en la sociedad tecnológica representa también para el ciudadano un menoscabo económico, pero también para sus derechos fundamentales.

Este tema debe posicionarse en el debate costarricense, se requiere que los ciudadanos y sus representantes asuman con responsabilidad la tarea de buscar una respuesta a estas interrogantes. No se trata sólo de encontrar el marco jurídico que permita el desarrollo de la personalidad virtual del ciudadano en una sociedad que se informatiza de manera tan acelerada, sino también que el ciudadano

no se vea expuesto, innecesariamente, a ataques informativos de particulares o del Estado mismo.

El filtrado de páginas peligrosas, la censura a la pornografía en los servicios institucionales, el filtrado de blogs y otros servicios se ha manifestado como una herramienta útil para incentivar de nuevo la concentración en el trabajo y para que los equipos institucionales no sean mal utilizados. Estas políticas, junto con líneas de seguridad en las empresas públicas y privadas, podrían ahorrar una gran cantidad de dinero en tiempo de trabajo perdido y en información afectada, robada y manipulada.

Lo interesante del ciberespacio es que este se extiende a todos los ámbitos de la vida de convivencia de los seres humanos: su hogar, su trabajo, sus relaciones íntimas. En todos esos ámbitos la promesa del ciberespacio es múltiple y al mismo tiempo la misma: la posibilidad de planificar una existencia a gusto, ya sea mediante un avatar que diseño a mi plena complacencia y que lo hago visitar mis sitios favoritos, ocultando mi verdadera personalidad.

El cambio de la política de seguridad debe ser sensible a estas formas de participación en los diversos ámbitos de vida ciudadana, y es aquí donde veo la importancia de fortalecer un régimen jurídico de la intimidad, no solo potenciando la personalidad virtual de los ciudadanos, sino también mecanismos y medios para que ellos puedan definir la forma y la intensidad de su interacción sin temor a intromisiones inadmisibles en sus derechos fundamentales.

Costa Rica ha avanzado en ambas líneas. Ya existen proyectos de ley muy maduros en el campo de la personalidad virtual y de la protección de datos personales, y es muy probable que esta nueva legislatura ponga atención a estos diseños normativos y los impulse como es debido. Es necesario crear las condiciones en las cuales un ciudadano pueda gozar de sus derechos y deberes en el mundo virtual, con un adecuado estándar de protección frente a los riesgos del ciberespacio y potencializando sus aportes al desarrollo económico y social del país. Si no se atienden estas necesidades individuales por más que se avance en un contrato social institucional y empresarial, el nivel de satisfacción humano será muy bajo.

Las empresas privadas norteamericanas, como lo revela el estudio citado de PriceWaterhouse and Cooper, tienden a tomar sus decisiones empresariales tomando en cuenta el impacto económico de pobres estándares de seguridad informática. Este criterio es mucho más importante y decisivo que por ejemplo tomar en cuenta la reputación de la empresa, el cumplimiento de la normativa vigente o acomodarse a las reglas internas corporativas.

Una primera aproximación a una política pública

Pienso que el diseño de políticas públicas requiere, en efecto, traducir esta actitud empresarial al sector público, pero con una dosis de atención al detalle humano y a los derechos fundamentales en juego. Se trata no sólo de ver el cálculo frío y numérico de las eventuales ventajas de obtener seguridad en el ciberespacio, sino también de tener ciudadanos en capacidad de ejercer sus derechos a la dignidad, a la intimidad, a la autonomía informativa y otras garantías individuales aun en ámbitos del ciberespacio. Es decir la posibilidad de un esquema "ganar-ganar" pasa de cerca de hacer consideraciones del nivel de protección de los ciudadanos y no en el mero bosquejo de políticas públicas de seguridad. Tanto el primer elemento como el segundo forman parte de la misma ecuación, y el Estado no puede olvidar que sin ellos cualquier acercamiento es miope y sin posibilidades de éxito.

También hay que educar y sensibilizar para una adecuada actitud en el ciberespacio. No se trata de asustar y ahuyentar a los ciudadanos del uso de nuevas tecnologías, lo que por otra parte creo que no se alcanzará. Se trata, a mi modo de ver, de sugerir formas de comportamiento que sean compatibles con esquemas de seguridad para sí y sus contactos.

Definiciones de la angustia

¿Cuáles son las definiciones de la angustia?

Después del 11 de setiembre los conceptos de ciberseguridad cambiaron porque después de este suceso se incluye dos concepciones, tanto preventivas como estratégicas, y el lenguaje utilizado es el que proviene de la guerra.

Es precisamente con este suceso histórico que empieza a desarrollarse, con más fuerza que nunca, una intentona legislativa para tratar de dotar de armas investigativas a los órganos del control penal y lograr con ello conjurar la amenaza del ciberterrorismo.

Sectores abarcados en USA

En Estados unidos los sectores abarcados por la temática de ciberseguridad pueden dar una idea de los grandes temas que tarde o temprano tendremos que asumir y revisar en nuestro país:

- Información y comunicación
- Transporte e infraestructura vial
- Energía y su distribución
- Banca y finanzas
- Aprovisionamiento

El sector salud no está abarcado pero es un tema que posteriormente se abarcó con la amenaza del ántrax, que afloró pocos días después del ataque a las Torres Gemelas en New York.

"Estrategia nacional para un ciberespacio seguro"

Luego del 2003, con la "Estrategia Nacional para un Ciberespacio Seguro"; y en la "Estrategia Nacional para la protección física de infraestructuras físicas y otras instalaciones clave" se incluyeron otros sectores a ser revisados:

- Agricultura y alimentos
- Banca y sector financiero
- Química y productos peligrosos
- Industria Militar
- Instalaciones sanitarias y de emergencia
- Energía
- Universidades
- Proceso penal

Esto para brindar mayor seguridad al país y para nutrir más a los organismos que responden de manera reactiva. La Casa Blanca nombró a

Ana Hathaway para que coordinara al país para protegerlo de ataques cibernéticos, eso cambió totalmente la política de Bush en el tema de seguridad lo que hizo él fue no tematizar el tema en público.

Un irrestricto control

Hay algo que quiero destacar en las políticas de Obama en contraste con las de Bush, mientras que este último no descartaba ningún medio para el combate del terrorismo y de la inseguridad, aun cuando tuviera que afectar derechos fundamentales, Obama busca revisar la política de ciberseguridad, de tal manera que valores trascendentes de nuestra cultura no se queden en el camino en la búsqueda de la huidiza seguridad que pretendía validar Bush con sus medios típicos del "Gran Hermano". Obama ha intentado desmarcarse de esa línea política y habrá que esperar a que su trabajo se manifieste en temas concretos.

Me parece que el tiempo y la coyuntura son proclives para el nacimiento del así denominado "ciberzar", quien tendría como tarea informar al Consejo de Seguridad y al Consejo Económico y no tanto al Presidente.

En el caso de Costa Rica deberíamos de involucrarnos activamente en una política de ciberseguridad, en donde destaque, en primer lugar, la definición y protección de la personalidad virtual de los ciudadanos, definir y enmarcar el entorno tecnológico del ciberespacio, la penetración tecnológica y los ámbitos que aun deben de ser fortalecidos para que más costarricenses gocen de los beneficios de la actual sociedad de la información. Junto a ello deben mapearse los ámbitos de peligro, la incidencia de la criminalidad informática, los medios utilizados e instrumentos a disposición, así como hacer estudios victimológicos de tal manera que puedan desarrollarse efectivas campañas de concientización y autoprotección. Al mismo tiempo deberíamos de revisar nuestras políticas institucionales y empresariales de protección de datos y crear la base legislativa, esperada desde hace tanto tiempo, para brindar a los ciudadanos garantías para el desarrollo de su personalidad y dignidad en los entornos virtuales. La mesa está servida para un interesante debate sobre el futuro del país en los nuevos dominios del ciberespacio.

Conceptualización de la ciberseguridad

Elena Gabriela Barrantes Sliesarieva

Se realiza una revisión de los conceptos básicos de seguridad. Asimismo, se tocan aspectos de implantación de seguridad y se ofrecen ejemplos de vulnerabilidades y defensas poco tradicionales.

Introducción

Usualmente se acepta que el objetivo de la ciberseguridad o seguridad informática es descubrir y aclarar la naturaleza de las amenazas y proveer metodologías para mitigarlas. Por lo tanto, al hablar de su conceptualiziaciòn, es indispensable definir las clases de amenazas, y las vulnerabilidades y ataques asociados a ellas. No hay que perder de vista, sin embargo que el alcance de cada uno de estos conceptos va a variar de acuerdo al contexto y a la aplicación en particular que se esté analizando.

Para iniciar, se define una amenaza como cualquier ocurrencia potencial, maliciosa o no, que pueda tener un efecto indeseable en los recursos de una organización. Una vulnerabilidad está siempre asociada a una amenaza y es básicamente cualquier característica de un sistema que permita (potencialmente) que una amenaza ocurra.

Claramente, al identificar y bloquear vulnerabilidades se logran mitigar las amenazas respectivas. Finalmente, un ataque involucra un ente malicioso que explota alguna vulnerabilidad para ejecutar la amenaza. Se puede ver un ataque como una instanciaciòn de una o varias amenazas.

Un ejemplo clásico de la interoperabilidad entre los tres conceptos presentados es el siguiente: una amenaza a un sistema es el robo de datos, y una posible vulnerabilidad es un sistema débil o inexistente de autenticación. Un ataque ocurre cuando un usuario conocedor de la vulnerabilidad en fortaleza de palabras de paso se matricula en el sistema y copia todos los datos a los que le da acceso la cuenta que rompió.

Para la construcción de la conceptualizaciòn iniciaremos con la clasificación de las clases básicas de amenazas, la idea de que la seguridad es una carrera armamentista con los atacantes, un recuento de las consideraciones básicas para implementar la seguridad, ejemplos de vulnerabilidades y de ataques, el concepto de análisis forense y una breve reflexión sobre la privacidad.

Clases de amenazas

Existen tres tipos básicos de amenazas: revelación de información, denegación de servicio, o repudio y corrupción de la integridad de los recursos (Amoroso, 1994). Otras amenazas que se van a tocar explícitamente, aunque sean instancias de la última clase son el secuestro del control y la suplantación. La relativa importancia de cada uno de ellos va a depender del sistema estudiado. Por ejemplo, en un sistema de telemedicina en tiempo real, una denegación de servicios representa una amenaza mucho más grande que la revelación de información.

La revelación de información se refiere a la amenaza de que un ente que no cuenta con autorización para el acceso a ciertos recursos, logra accederlos de forma indebida. Un ejemplo es el acceso de un ladrón al número de una tarjeta de crédito ajena, pero también al acceso no autorizado de una compañía de datos personales de ciudadanos con los que no posee ninguna relación legal.

La denegación de servicio, o repudio corresponde a la amenaza "inversa": que los entes que sì cuentan con autorización de acceso a los recursos no consigan entrar (esto es, sean repudiados a la entrada). Por ejemplo, la amenaza de que los usuarios no logren navegar en el sitio web de una empresa debido a que el servicio de nombres (DNS) esté atascado por solicitudes mal formadas.

La corrupción de la integridad es intuitivamente la más "agresiva", ya que se trata del acceso directo a los recursos, y como individuos con mayor o menor grado de territorialidad, es la que despierta mayor grado de rechazo. Sin embargo, se debe recordar que las amenazas no viven en el vacío. Si el recurso indebidamente modificado es de poco valor para la organización, quizás una preparación demasiado reactiva ante esa amenaza sea contraproducente.

La amenaza de corrupciòn de integridad comprende muchos aspectos, más allá de la definición de daño, pérdida o inserción de información falsa. En particular se quiere resaltar dos de ellos: el secuestro de control y la supantación de identidad, ambas amenazas muy reales actualmente. Es fácil imaginarse las consecuencias de que un atacante esté controlando su máquina, que puede ser el servidor corporativo o su laptop, y que además esté utilizando sus datos para realizar transacciones.

La carrera armamentista en ciberseguridad

Claramente las vulnerabilidades que permiten la ocurrencia de ataques y los detalles de los mismos dependen enteramente de cada sistema. Sin embargo, es posible identificar tendencias, y una de las más interesantes es lo que se puede denominar una carrera armamentista, muy similar a la que ocurre en la naturaleza a múltiples niveles, por ejemplo con los virus.

Cuando un organismo vivo es atacado por un virus, este eventualmente logra bloquear alguna de las vulnerabilidades que permiten el ataque, por ejemplo modificar un camino químico que le impide al virus reproducirse en el organismo. Sin embargo, rápidamente aparece una mutación del patógeno que evade la defensa y utiliza alguna vulnerabilidad alternativa. Por cuanto los organismos vivientes son sistemas muy complejos, este tipo de interacciones pueden seguir operando para siempre.

En el caso de los sistemas computacionales, la situación es muy similar a la descrita previamente. Son sistemas complejos, en constante evolución: algunas vulnerabilidades se bloquean, pero otras aparecen al modificar el software, y los atacantes se adaptan. Es poco probable que esta tendencia cambie en algún momento.

Es también importante aclarar que el tema de la seguridad ha sido una preocupaciòn de los diseñadores y operadores de sistemas informáticos desde su inicio. Por ejemplo, en 1974 se publica un reporte técnico que describe un proceso de análisis de vulnerabilidades en un sistema Multics, mediante un test de penetración., y muchas de las clases de vulnerabilidades y ataques que proponen, descubren o usan, conceptualmente aún están siendo utilizadas. Este es el caso del ataque que llamaremos por extensión de buffer overflow, que depende de las siguientes vulnerabilidades genéricas: (a) errores u omisiones en el procesamiento de datos de entrada que (b) permiten modificar apuntadores de uno u otro tipo que (c) hacen posible modificar, leer o bloquear el acceso a datos que no estaban dentro del alcance del usuario o programa que realizó originalmente la entrada de datos (Karger, 1974). A pesar de los grandes cambios que se han dado en la computación hasta este momento siguen existiendo ataques reales que, a nivel de concepto siguen estando emparentados con el buffer overflow.

La tendencia es entonces a que se cierra un portillo y aparecen muchos más. Esto se ve reflejado tanto en el creciente tamaño de las conferencias técnicas en seguridad como en el tamaño de las Bases de Datos utilizadas por los antivirus y otros programas de seguridad para filtrar la información que entra a los sistemas.

Algunas consideraciones para implementar la seguridad

Uno de los aspectos más importantes a rescatar es que la seguridad debe estar incorporada desde el diseño, para minimizar el número de vulnerabilidades, y que permita arreglarlas cuando se descubran de una manera más metódica y completa. Otro es que se debe aceptar que no existe ningún sistema completamente seguro y planificar de forma acorde. Finalmente, bajo ninguna circunstancia se debe usar seguridad por oscuridad, dado que los atacantes rápidamente

descubrirán sus vulnerabilidades, pero los defensores no contarán con el beneficio de una comunidad grande organizada trabajando en detectar vulnerabilidades y reportarlas rápidamente, y con apoyo para mejorar el software incrementalmente.

Es importante no perder de vista que la seguridad siempre implica un compromiso con la usabilidad. Este compromiso implica que para implantar una seguridad efectiva, se debe estar dispuesto a negociar con las comunidades involucradas dentro de la organización, dado que existe una tendencia general a subestimar los costos de no implementar medidas de seguridad, lo que redunda en resistencia a pagar los costos de implantación. Para vencer esta resistencia al cambio a todos los niveles se pueden usar varias tácticas, pero -aunque efectivo- es poco recomendable utilizar demostraciones en vivo de ataques, por cuanto se pueden perder o revelar datos reales, o darle demasiada información a entes externos.

Una consideración significativa es que los usuarios tienden a recordar los errores pero olvidarse de los éxitos, así que una solución implementada con poco cuidado puede deshacer meses de cuidados trabajo de convencimiento, por lo que es altamente recomendable siempre realizar la evaluación de riesgos y el análisis costo-beneficio, antes de intentar convencer a la organización.

Ejemplos de vulnerabilidades

En esta sección se ofrecen algunos ejemplos específicos de vulnerabilidades. El primer ejemplo es sobre los canales ocultos. Aún en un ambiente donde toda la información explícita esté protegida (por ejemplo, todos los archivos son inaccesibles desde el exterior y los mensajes viajan cifrados), algo de la información sobre el sistema se fuga. Por ejemplo, un atacante puede contar mensajes, o ver de donde vienen y para donde van, o medir el tiempo entre paquetes. Esta información “filtrada” se denomina “canales ocultos”, y existen en múltiples puntos de los sistemas. Se han dado ataques reales exitosos utilizando información tan pública como la que se está presentando. Así que suponer que toda la información está protegida solo porque los datos estén ocultos es claramente peligroso.

Otra fuente de vulnerabilidades son los esquemas de cifrado, que pueden tener problemas de implementación (varios ataques aprovecharon esto) o problemas de fondo, como tamaño de la llave, supuestos de los algoritmos etc. El problema es que típicamente los sistemas de cifrtado son complejos de por sí, y es realmente difícil visualizar estas vulnerabilidades.

Por mucho, la forma más fácil de robo de datos es la ingeniería social. Por ejemplo, de nada sirven múltiples sistemas de seguridad si un empleado que está legítimamente autorizado a usar un sistema se lleva los datos y los vende a un tercero.

Finalmente hay que considerar las potenciales vulnerabilidades de los sistemas sobre los que corren las aplicaciones y sobre ls que se tiene poco control, como errores en el hardware, el sistema operativo o la plataforma de programación. Para considerar estos casos hay que mantenerse al día con los parches respectivos y programar aplicaciones de forma paranoica, sin confiar en nada obtenido del sistema hasta no revisarlo.

Ejemplos de defensas

Existen cada vez más formas de protección de datos, y decidir entre ellas es complejo. Parte de la solución está en establecer defensas en profundidad en lugar de desechar una para instalar otra. Para herramientas cuyo objetivo sea el mismo (por ejemplo, los antivirus), se debe estar monitoreando constantemente las actualizaciones Asimismo, si es posible, se debe establecer diversidad, contando con dos o más productos equivalentes simultáneamente implantados en la red.

Otra manera de aumentar la diversidad, lo que aumenta la resistencia a los ataques es utilizar diferentes tipos de defensa: tanto estáticas como adaptativas. Un ejemplo de sistemas adaptativos son los nuevos sistemas de detección de intrusos. La ventaja es que estos sistemas cuentan con procesos de aprendizaje por lo que no dependen de constantes actualizaciones de la base de datos. El problema es que al haber mucho ruido en la señal (distinción entre propio y ajeno), muchas veces se disparan demasiado

o insuficientemente, y ambos casos son peligrosos. Es por esto que los sistemas adaptativos siempre deben tener algún grado de supervisión y soporte con sistemas estáticos.

Un caso interesante de un sistema estático pero no dependiente de patrones es la introducción de ruido semi-aleatorio para perturbar las máquinas de inferencia de los canales ocultos. Por ejemplo si el atacante está tratando de adivinar la estrategia que se está usando para asignar reservaciones, unas cuantas transacciones fantasmas al azar pueden perturbar lo suficiente al mecanismo del atacante como para que no logre efectuar la deducción.

Análisis forense

El análisis forense es muy útill para determinar de la forma más exacta posible cómo sucedió un ataque para poder encontrar las vulnerabilidades que este aprovechó y cerrarlas, pero al mismo tiempo para evaluar la extensión del daño y tratar de mitigarla.

Privacidad y seguridad

Este es un tema largo e importante, pero al menos debe quedar claro que ninguna conceptualizaciòn de la seguridad es completa sin tocar aspectos de protección de datos de los usuarios finales, y nuestro país tiene grandes lagunas legales y de concientización al respecto. Por ejemplo, el correo electrónico es totalmente “abierto” a menos que se cifre de punto a punto, pero muchos usuarios ignoran esto y lo usan como si fuera totalmente secreto con resultados a veces trágicos.

Todos y todas debemos informarnos, informar a los demás, y mantenernos alertas sobre la tecnología que usamos, la protección de la que disponemos y sobre la visibilidad de nuestros datos en Internet.

Robo de identidad y el Vector-Personal

Oldemar Rodríguez Rojas

Uno de los problemas más serios de muchas instituciones bancarias a nivel mundial es el fraude mediante el robo de identidad, es el caso de las tarjetas de crédito y en el fraude en llamadas telefónicas. Más serios porque, por ejemplo, de 80.000 mil transacciones diarias en un banco apenas 3 o 4 suelen ser fraude, lo cual hace sumamente difícil su detección, sin embargo, algunas veces estos 3 o 4 fraudes pueden representar una pérdida de más de 25 mil dólares.

El Vector-Personal es un método matemático para detectar atipicidad en el comportamiento de algo o alguien (puede ser una persona o incluso una máquina la que se aparta de su patrón habitual de comportamiento o funcionamiento). La atipicidad está expresada por aquellos cambios que un individuo presenta en su conducta normal a lo largo de un período de tiempo. Existen muy diversas razones de oportunidad o de riesgo por lo cual es sumamente importante en banca y en otros negocios detectar aquellas transacciones que se apartan de una conducta habitual. Problemas como la detección en línea de fraudes en tarjetas de crédito o débito, la atipicidad en el uso de las cuentas corrientes, transacciones atípicas por Internet y fraudes en llamadas telefónicas, son ejemplos de uso de esta tecnología.

La idea central del Vector-Personal es sustituir el conjunto de todas las transacciones realizadas por una persona (u objeto cualquiera) por una sola "transacción" que resume todas las originales (Vector-Personal), de manera que se podrían resumir millones de transacciones en una sola que conserva la conducta habitual del cliente. Esto se logra gracias a que esta nueva transacción tendrá en sus campos no solamente números (como en las transacciones usuales), sino que podrá también tener objetos tales como intervalos, histogramas o reglas.

Si se tiene, por ejemplo, una tabla con transacciones, en cada una de ellas está el código individuo, la edad, la profesión, el sueldo y la provincia. Si en este caso se decide construir un Vector-Personal por cada provincia. Entonces si la edad en San José se representa por el intervalo [36,39] que son las edades mínimas y máximas respectivamente en San José (presentes en la tabla original), esto significa que la edad de cualquier persona que viva en San José estará comprendida entre 36 y 39 años. Mientras que la profesión en San José está representada por un histograma que dice que la mitad de las personas de la tabla original son abogados y la otra mitad son doctores.

El Vector-Personal es entonces un arreglo de números, intervalos, histogramas y/o reglas que permiten resumir la conducta de un objeto o persona, el cual es construido a partir de una base de datos de transacciones realizadas por esta persona u objeto.

Aún cuando algunos ya habían sugerido ideas similares en el pasado, su implementación computacional había sido imposible ya que; por ejemplo, cuando una persona hace una compra con su tarjeta, el computador autorizador tiene solo 30 segundos para procesarla y de no responder la máquina la dará por buena. Imposible porque en 30 segundos no se puede recorrer una base de datos de millones de registros para verificar si el cliente hace este tipo de compras o no.

Aquí es donde radica la importancia del Vector-Personal, ya que gracias a este es posible almacenar en un vector de tan solo aproximadamente 28k bytes de memoria toda la conducta (perfil) de un cliente. Esto ya que no se almacenan números (como es lo usual) sino símbolos que resumen la conducta, por ejemplo, con un histograma

se puede resumir fácilmente las horas más frecuentes de compra usadas por un cliente. Gracias a que este Vector-Personal es tan pequeño, la comparación para ver, por ejemplo, si el tarjeta-habiente se está apartando de su patrón tarda apenas 8 milisegundos.

Problema del fraude en tarjetas de crédito o débito

Cuando una persona hace transacciones en un banco, en un cajero o en un comercio, dicha transacción se traslada a una base de datos y luego usualmente algún sistema informático las analiza y para aquellas que encuentra sospechosas de fraude envía una alerta a un departamento de análisis del fraude. En este departamento se encuentra un grupo de personas que las analiza y de confirmarse la sospecha el tarjetahabiente es llamado, usualmente vía telefónica, si este confirma el fraude la tarjeta es inmediatamente suspendida.

El problema radica en que una persona de estas puede analizar unas 500 transacciones al día, si el banco tiene un departamento de detección del fraude con 5 empleados, entonces podrá analizar únicamente unas 2.500 transacciones al día. Tomando en cuenta que un banco de tamaño mediano tiene unas 80.000 transacciones de tarjeta al día, esto resultará insuficiente si no se tienen muy bien escogidas las alertas que van al departamento de detección del fraude.

La mayoría de los sistemas informáticos tratan de buscar el fraude mediante la búsqueda del *patrón del fraude,* esto usualmente se hace con Reglas de Experto o que un método conocido como Redes Neuronales. El problema que tienen todos estos sistemas es que el patrón del fraude realmente no existe, porque de cada 80.000 transacciones usualmente solo unas 3 son fraude, por lo que el patrón de estas 3 transacciones se repite en cientos de transacciones que no son fraude, de manera que si alertan todas las transacciones con este patrón se tendrían entonces demasiadas alertas falsas en el departamento de monitoreo del fraude.

Nuestra propuesta, consiste en detectar el fraude de una manera completamente diferente, esto es, buscar el fraude buscando aquello que el tarjetahabiente jamás haría con su tarjeta. Es decir, buscar aquellas transacciones que son atípicas para el dueño de la tarjeta.

Nuestro método ha resultado sumamente exitoso porque las personas hacen muy pocas transacciones atípicas, alrededor de un 2% de sus transacciones, lo que permite que el nivel de alertas en el departamento de detección de fraude del banco sea muy bajo. Además cuando un ladrón roba una tarjeta, en su afán de robar rápido la mayor cantidad de dinero, efectúa transacciones que son, en su mayoría, atípicas para el dueño de la tarjeta. Así aproximadamente el 97% de las transacciones fraudulentas son atípicas, lo que permite una detección muy alta del fraude.

El problema es entonces como detectar la atipicidad. Para esto tenemos que tener almacenado el perfil o patrón de compra de cada uno de los tarjetahabientes. Dicho perfil se encuentra en el historial de compra del cliente, pero para poder consultarlo en línea se requiere de almacenarlo de manera muy eficiente. Es ahí donde surge la idea de utilizar el Vector-Personal para almacenar dichos perfiles de compra. El Vector-Personal se convierte en le "ADN" del cliente, en el sentido de su patrón de compras.

Para detectar la atipicidad, el Vector-Personal incluye un campo que es la máxima distancia histórica del cliente, la cual significa lo más que un cliente se ha alejado de su perfil de compra en toda su historia como cliente. Cuando una nueva transacción se aleja más que esto entonces una alerta es enviada al departamento de detección del fraude del banco y por ende al cliente. Por el contario cuando la distancia de la transacción no es más grande que este máximo histórico entonces la transacción se considera típica y no se manda ninguna alerta.

De manera similar el Vector-Personal ha sido utilizado para detectar fraude en llamadas telefónicas, detectar lavado de dinero y en muchas otras aplicaciones en las que se desean detectar comportamientos atípicos.

Bibliografía

Billard, L. and Diday E. Symbolic data analysis: Conceptual statistics and data mining. Wiley, New York, 2006.

Bock H-H. and Diday E. (eds.) Analysis of Symbolic Data. Exploratory methods for extracting statistical information from complex data. Springer Verlag, Heidelberg, 425 pages, ISBN 3-540-66619-2, 2000.

Cazes P., Chouakria A., Diday E. et Schektman Y. Extension de l'analyse en composantes principales à des données de type intervalle. Rev. Statistique Appliquée, Vol. XLV Num. 3., pag. 5-24, Francia, 1997.

Chouakria A. Extension des méthodes d'analyse factorielle à des données de type intervalle. Thése de doctorat, Université Paris IX Dauphine.

Diday E. and Rodríguez, O. (eds.) "Workshop on Symbolic Data Analysis". PKDD–Lyon-France, 2000.

Groenen P.J.F., Rodríguez O., Winsberg S. and Diday E. IScal: Symbolic Multidimensional Scaling of Interval Dissimilarities. In COMPUTATIONAL STATISTICS & DATA ANALYSIS the Official Journal of the International Association for Statistical Computing, Vol. 51, Nov. 2006.

Meneses E. and Rodríguez O. Using symbolic objects to cluster web documents. 15th World Wide Web Conference, 2006.

Rodríguez O. Classification et Modèles Linéaires en Analyse des Données Symboliques. Thèse de doctorat, Université Paris IX Dauphine, France, 2000.

Rodríguez O. The Knowledge Mining Suite (KMS). Publicado en ECML/PKDD 2004 The 15th European Conference on Machine Learning (ECML) and the 8th European Conference on Principles and Practice of Knowledge Discovery in Databases (PKDD), Pisa Italia, 2004.

Rodríguez O., Diday E. and Winsberg S. Generalization of the Principal Components Analysis to Histogram Data. PKDD2000, Lyon-France, 2000.

Rodríguez O., Castillo W., Diday E. and González J. Correspondence Factorial Análisis for Symbolic Multi–Valued Variables. Subjected for publication in Journal of Symbolic Data Analysis, 2003.

Rodríguez O. and Pacheco A. Applications of Histogram Principal Components Analysis. Publicado en ECML/ PKDD 2004 The 15th European Conference on Machine Learning (ECML) and the 8th European Conference on Principles and Practice of Knowledge Discovery in Data bases (PKDD), Pisa Italia, 2004.

Capítulo 2
Ciberseguridad y privacidad

Seguridad y autodeterminación informativa

Marvin Carvajal Pérez

Uno de los aspectos centrales de la protección de datos, quizá uno de los menos tratados en nuestro país por parte de los órganos que han conocido de esta materia es el tema de la seguridad.

Privacidad se dice en todo caso con alguna indulgencia, pues no se considera que únicamente se está ante una situación relacionada con los datos privados e íntimos de la persona, sino de cualquier información de carácter personal, incluso cuando no tenga esa connotación de privacidad.

Para abarcar el tema, básicamente hay 5 aspectos fundamentales, primero a la seguridad de la información, segundo, la seguridad de la autodeterminación informativa, tratando de relacionar ambos conceptos, qué se ha hecho en el derecho comparado en relación con esta materia, qué se ha hecho y qué se está haciendo en nuestro país, para así finalmente tratar de llegar a una conclusión.

Sobre el tema de la seguridad de la información, es conocido que los tres grandes principios, los tres grandes objetivos de cualquier sistema de seguridad, no solamente los informáticos, sino incluso para la seguridad de los archivos físicos.

Primero, lograr la confidencialidad, que no hayan intrusiones, que no se den fugas de información, que la información no sea finalmente accedida por personas no autorizadas para ello.

Segundo la integridad que la información pueda ser conservada; que esta pueda mantenerse de manera incólume, que no sea alterada, que no sea sustraída, que no sea dañada, que no sea desactualizada, es decir, una serie de medidas para lograr que la información no sea alterada de manera que no corresponda efectivamente a la realidad.

Finalmente, la disponibilidad, que se manifiesta en medidas tendientes a que la información pueda estar siempre en nuestras manos, para que podamos consultarla utilizarla de la manera más adecuada.

Seguridad de la información

Medidas de seguridad

En principio, todo sistema de seguridad debería responder a esos principios. Normalmente, se atiende a esta necesidad de garantizar la seguridad con al menos tres tipos de medidas:

- Medidas de carácter jurídico. Normas generales, normas internas de seguridad, protocolos, etc.
- Medidas de carácter técnico. Defensa en profundidad (cor tafuegos, antivirus, reglas de acceso, claves complejas, encriptación, registros de uso, respaldos, etc.)
- Medidas de carácter organizacional. Distribución clara de responsabilidades, sensibilización, capacitación.

De carácter jurídico para empezar los Estados emiten normas generales tanto para la protección de los datos personales, como específicamente para la regulación de la seguridad de la información constante en diversas bases de datos; se emiten normas internas de seguridad, sea en instituciones públicas u organismos privados; se emiten protocolos con la forma de cómo será manejada la información, cómo será custodiada, la forma en que será accedida, cómo será manipulada y todas estas normas tienden a garantizar la seguridad de la información.

Medidas de carácter técnico. A partir del concepto de defensa en profundidad e implica el establecimiento contra fuegos, antivirus; la emisión de reglas de acceso, claves complejas, encriptación de la información particularmente cuando está es trasladada, transferida o manipulada de alguna forma, registros de usos, bitácoras, respaldos, etc. Es decir, hay una serie de medidas tecnológicas que pueden ser adoptadas para favorecer la seguridad de la información.

Organizacionales como por ejemplo una distribución muy clara de responsabilidades en manejo de la información, sensibilización al personal acerca de cuáles son las consecuencias de hacer un uso inadecuado de la información que obre en sus registros y por supuesto la capacitación esencial.

Seguridad y autodeterminación informativa

¿Por qué relacionar el tema de la seguridad de la información con el derecho a la autodeterminación informativa?

El derecho a la autodeterminación informática ha sido reconocido y desarrollado contundentemente por parte de la Sala Constitucional, como un derecho fundamental de toda persona a que su información sea procesada, sea manipulada de manera legítima, en forma acorde con sus derechos, de manera tal que la persona no se vea limitada con el ejercicio de su propia libertad por temor a encontrarse vigilada, por temor a que esa manifestación de su libertad le traiga en determinado momento consecuencias negativas.

La seguridad en sí es un elemento del derecho de la protección de datos personales, del derecho a la autodeterminación informativa, así como es reconocido por nuestra Sala Constitucional; así es regulado por los países que cuentan con una normativa relacionada con la protección de datos personales y es considerada en todo caso un elemento intrínseco del derecho a la autodeterminación informativa.

Segundo, porque la seguridad dificulta el acopio ilegitimo de la información. Cuanto más segura sea la forma en que es manipulada la información, tanto más se evitará que esta sea captada por fuentes de una manera ilegítima.

Una fundidora que recepta medidores robados del Instituto Costarricense de Acueductos y Alcantarillados para convertirlos en láminas de metal, esta actividad que pareciera totalmente legítima, está alentando una actividad delictiva de enorme gravedad para el país. Cada vez una chatarrera recibe la tapa de una alcantarilla sustraída, está poniendo en peligro la vida de una persona, está poniendo en peligro los servicios públicos, si se recepta cable o cualquier otro de este tipo de bienes, sucede exactamente lo mismo con la información.

La seguridad no es una regla exclusiva de algunos determinados tipos de empresa que manipulen información, la seguridad es una regla que va dirigida a todas las instancias que de una u otra manera tengan bases de datos con información personal, ya que la sustracción de manera ilegítima y el uso de la información sustraída, constituyen el mismo tipo de delito, no está tipificado como tal y esta es una de las limitaciones del derecho penal, pero tiene la misma gravedad, es un mal social de la misma gravedad que la aceptación de cable robado del aeropuerto Juan Santamaría, que la admisión de una tapa de alcantarilla de la calle principal de Curridabat, es exactamente el mismo tipo de delito. De ahí que la seguridad incida directamente en dificultar que se acopie de modo ilegítimo la información.

Incide directamente en la calidad de la información la autodeterminación informativa, porque la información que obre sobre nosotros en las bases de datos debe de ser de calidad, debe ser veraz, exacta, actual; un mal manejo de la seguridad puede incidir en que no se logre manipular información de esa naturaleza. Simplemente porque para tener información veraz, exacta y actual, debemos garantizar la integridad de esta información, que no sea objeto de intrusiones ilegítimas, que no esa objeto de pérdidas de información, etc.

También es muy importante porque determina las reglas de transferencia de la información. La regla de principio es que el traslado de la información de una base de datos a otra tiene que darse entre partes que cumplen con reglas relacionadas con la protección de datos personales y una de ellas es la regla de la seguridad. Violamos o lesionamos tanto este derecho cuando utilizando inadecuadamente la información, como trasladando la información de una base

segura a una base insegura; en ambos casos, estamos poniendo en peligro a las personas al hacerlo.

Regulación comparada

Refirámonos un poco a la regulación comparada. Como ustedes saben, nuestro país no cuenta con una legislación especial para la protección de datos personales. En tres períodos constitucionales distintos, desde finales de los años 90, se están paseando por la corriente legislativa, que no es tan torrentosa como su nombre lo quiera indicar, diversos proyectos de ley tendientes a la regulación de los datos personales; sin embargo, ninguna de estas leyes ha sido aprobada hasta el momento, pese a que otros países hermanos sí cuentan con regulación de esta naturaleza.

Argentina tiene una ley del 2000. Argentina que es el único país de América Latina considerado como poseedor de un nivel adecuado de protección por parte de la Unión Europea. Dicha ley en su artículo 7º regula la confidencialidad de la información como exigencia para las personas que se desempeñen en una base de datos de esta naturaleza; en artículo 21.2 inciso g, los medios de seguridad son regulados; se determina que todas las bases de datos públicas y privadas dispongan de medidas de seguridad.

En el caso argentino, además, en la disposición 9 – 2008, que es un reglamento, creado a partir de una directriz emitida por la Dirección de Protección de Datos Personales, en la cual se refiere de manera expresa a las medidas de seguridad de las bases de datos públicas y privadas. Este reglamento argentino, fundamentalmente lo que hace es establecer niveles de seguridad: un nivel mínimo, un nivel medio, un nivel crítico; las reglas para cada uno de estos niveles de seguridad, el procedimiento que se debe seguir en cada caso para establecer dichas medidas y las responsabilidades que atañen a cada persona que administren estos ficheros de esta naturaleza.

México que tiene una ley no especializada en la protección de datos personales, sino que es una ley más bien de acceso a la información pública, pero que también regula el tema de la autodeterminación informativa, una ley de 2002, la cual establece en el artículo 20

inciso 6 el deber de establecer medidas que eviten la acción de alteración, pérdida o uso indebido en bases de datos que consten en entidades públicas y privadas.

Chile también tiene una regulación de 1999, la cual reconoce el principio de confidencialidad y en el artículo 11, el deber de cuidado de la persona responsable del fichero. Paraguay tiene una norma de 2000; sin embargo no regula directamente el tema de la seguridad.

Perú tiene una ley de 2001, que en el artículo 12 establece amplios niveles de seguridad, pero que están restringidos a las centrales de riesgo, a las protectoras de crédito, lo que es muy limitante para lo que se quiere lograr a través de la autodeterminación informativa. El riesgo de la manipulación de la información no está únicamente en estas protectoras de crédito; está en cualquier instancia pública o privada, está en un banco, en un hospital, en una escuela pública que maneja información que nos pertenece, el video club al que estamos afiliados.

Uruguay tiene una ley del 2004, que en su artículo 7 se refiere a la confidencialidad de las personas que se desempeñen en un fichero.

Regulación comparada España

El país de tradición latina con una regulación más acentuada en este tema, junto con Italia es España.

España tiene una ley de 1999 en cuyo artículo noveno establece un deber de seguridad contra la alteración o tratamiento basado en un acceso no autorizado. Toma en cuenta el Estado de la tecnología, es decir, se trata de una norma progresiva, que es un término que se utiliza en derechos humanos, es decir, en cuánto más aumente la capacidad tecnológica para fomentar o ayudar a los niveles de seguridad, mayor debe ser el esfuerzo de estas bases de datos para garantizar esta seguridad. No pueden utilizarse los remedios del 99 para curar las enfermedades del 2009.

Igualmente toma en cuenta el estado de la tecnología, el tipo de información de que se trate, por ejemplo, no podemos tratar igual la pertenencia a una asociación comunal de vecinos, que la afiliación a una asociación religiosa, mezclar la pertenencia de una de estas

sociedades religiosas con los datos médicos, etc. La ley española toma en cuenta y valora en forma especial los riesgos que pueda generar el uso indebido de diferentes tipos de información. El artículo 11 establece el deber de secreto de los funcionarios que se desempeñen en las agencias de acopio y manipulación de datos.

España también produjo un reglamento en 1999, el 994, sobre medidas de seguridad en ficheros automatizados. La protección de los datos personales no se restringe a la protección de los ficheros automatizados, la información que esté impresa en un archivador metálico puede, a través de un mal manejo de la misma, perjudicarme tanto como aquella contenida en una base de datos electrónica; por supuesto que la posibilidad de que me generen daño en una base de datos electrónica es mucho mayor.

Podemos mencionar, en relación con este reglamento español, que al establecer una regulación parecida a la argentina que les mencionaba, crea una obligación para las empresas que manejan información y es crear un documento de seguridad. Cada una de estas empresas tiene que establecer un protocolo de actuación en materia de seguridad, este instrumento es luego controlado por las autoridades públicas, lo cual resulta de mucho interés con miras a la futura regulación nacional en la materia.

En España la agencia para la Protección de Datos Personales ha conocido muchos casos relacionados con la seguridad; la Agencia es una instancia administrativa que controla el buen manejo de los ficheros públicos y privados y su adecuación a las reglas de protección de datos personales y hay una vasta producción de resoluciones de esa agencia dos ejemplos.

La resolución 0097 de 2009 contra la Universidad Estatal a Distancia llamada la UNED también en España. La Universidad en ese caso tenía un fichero relacionado con la discapacidad que tenían varias personas. Este fichero de personas discapacitadas tenía una finalidad totalmente legítima, conceder becas a quienes padecieran de una discapacidad, para lograr así que pudieran concluir más eficazmente con sus estudios; además, para adecuaciones curriculares, tenía una serie de aplicaciones. Lo que pasa es que se descubrió que

este fichero que contenía información tan sensible, se encontraba ubicado en el mismo lugar de la relativa a los estudiantes que no tenían estas características; no se había individualizado esta información o separado en un compartimento aparte más seguro, pese a ser información altamente sensible para estas personas.

La resolución 161 contra el servicio público de empleo de Castilla La Mancha. En este caso, es muy interesante para observar la intensidad del control que tiene la Agencia sobre las bases de datos en España. Se determinó que datos que la gente había aportado a la seguridad social, el equivalente al Caja Costarricense de Seguro Social en Castilla La Mancha, habían sido transferidos al Servicio Público de Empleo de Castilla La Mancha, que es una organización relacionada con la administración de la carrera en el servicio público. Hasta ahí íbamos muy bien, pero se logra determinar que se habían dado intrusiones ilegítimas a esa base de datos; que personas no autorizadas se había aprovechado de esa información del Servicio Público de Empleo de Castilla La Mancha para entrar y acceder a datos que habían sido entregados a la Seguridad Social.

En ambos casos, la Agencia de Protección de Datos Personales condenó fuertemente a las empresas, estableciendo precedentes muy relevantes en esa materia.

Regulación nacional

Regulación nacional en esta materia, no tenemos. Carecemos una ley general en relación con la protección de datos personales; esto ha tenido que ser suplido por la jurisprudencia constitucional, la cual se ha mostrado muy creativa en esta materia.

Algunas personas podrían considerar que la Sala se ha convertido en un legislador positivo en esta materia; es decir, en un creador de normas jurídicas a través de la jurisprudencia, un creador pretoriano de normas. Sin embargo, debemos decir que no existen resoluciones especializadas sobre el tema de seguridad; no es el aspecto más fácilmente comprendido por quienes nos dedicamos al área del derecho y al tema de la protección de derechos fundamentales.

Sin embargo, hay resoluciones directamente relacionados con este tópico, como las que se refieren a las reglas de calidad a que hacíamos referencia hace algunos minutos, así como a la transferencia de la información. Podríamos así afirmar que existe una plataforma normativa para asegurar que la seguridad que se maneja en las bases de datos, como parte fundamental del derecho a la autodeterminación informativa, reconocido por la Sala Constitucional y esto puede tener mucho peso ante una mala utilización de estos datos.

Hay diversos proyectos de ley que han pasado por la corriente legislativa. De estos cabe destacar el proyecto de ley de "Derechos de la persona frente al tratamiento de sus datos personales" en diminutivo la ley PRODAT, el cual prevé en el artículo 7º la seguridad de los datos, tanto en las medidas que se deben adoptar para obtener la información, como en relación con las capacidades tecnológicas en el momento, también prohibiendo que sean registradas las informaciones en bases de datos no seguras, permitiendo que por vía reglamento se establezcan normas ágiles para la salvaguarda de la información y estableciendo responsabilidades concretas a quienes tengan a su cargo dichos ficheros.

Conclusión

La implementación de reglas y procedimientos seguros en el acopio, almacenamiento y transferencia de datos personales repercute directamente en el respeto al derecho fundamental a la autodeterminación informativa.

Podríamos concluir, a partir de lo que les he mencionado en estos minutos, que la implementación de normas y procedimientos seguros en el acopio, almacenamiento y transferencia de datos personales incide directamente en el respeto a un derecho de rango constitucional, como es el derecho a la autodeterminación informativa, reconocido por la Sala Constitucional en una muy basta doctrina jurisprudencial.

Es sin duda alguna una preocupación que debe estar presente en aquellas bases de datos creadas para ofrecer informes al público, pero debe serlo en todas y cada uno de los ficheros que manejen información personal, puesto que de estas se alimentan las otras

bases de datos para dar esos informes. Es decir, es una regla general del sistema que debemos tomar con el mismo cuidado que para administrar los fondos de una cuenta nuestra, con el mismo cuidado debe ser administrada la información personal que nos pertenezca y que obre en las bases de datos públicas y privadas.

Esto es, sin duda alguna, un aspecto muy relevante de la autodeterminación informativa, un elemento muy relevante en la protección de datos que atañe a los derechos de la persona frente a este mundo tecnológico que avanza cada día más en ofrecernos nuevas alternativas de comunicación, nuevas alternativas de conectividad y por supuesto, nuevos riesgos de los cuales debemos protegernos con firmeza.

El Derecho a la información

Federico Malavassi Calvo

Estamos ante este tema para entender cuál es la legislación, si es que la hay, o cuáles son algunos de los principios jurídicos aplicables porque precisamente estamos en temas vivos o en algunos casos si valen las mismas reglas de antes.

Un delito aunque no esté tipificado, hay conductas dañinas en algunos hechos aunque no estén tipificadas en el derecho y en el derecho jurídico no hay pena y no hay delito si no hay tipificación y buena parte de la labor de los *hackers* es dañina y no aparece como delito.

Para desconsuelo de todos ustedes les cuento, que hace más o menos 4 años estuvimos tratando de sacar un nuevo código penal que llevaba al menos 10 años dando vueltas de la seca a la meca, cada vez que iba a la corte se le perdía una página y cada vez que volvía a la Asamblea se le perdía otra página y cuando me encontré el artículo relativo a delitos informáticos a alguien se le había ocurrido colectar una serie de verbos nada más divididos por comas, a quién corte, pegue, agregue o quite, contradictorios sin entender realmente cuál era la acción típica que había que analizar.

En el caso que estamos hablando de la privacidad precisamente tenemos ese tema, una actividad social que avanza en física quántica

por decirlo así, porque ya avanza en quánticos y una actividad jurídica que va muy atrás. Y no sólo va muy atrás ni siquiera entiende lo que está pasando.

Los que somos profesores universitarios por lo menos una vez al semestre, una vez al cuatrimestre, levantamos una base de datos con nuestros alumnos y normalmente pedimos algo más que el nombre, pedimos un correo, pedimos un teléfono y quienes hacemos con alguna pasión la actividad de la enseñanza ponemos algunas cosas más, ponemos una dirección, ponemos algún detalle, ponemos alguna otra cuestión y empezamos a alimentar una pequeña base de datos. ¿Qué pasa al final del semestre o del cuatrimestre? Pues algunos lo tenemos allí en algunos archivos, muchos sencillamente los desaparecemos y muchos ni saben que suceden con esas cosas. Lo que se nos está diciendo ahora es que todos tenemos responsabilidad por esos datos.

La autodeterminación informativa

Hay una precisión que quería hacer sobre el tema de la autodeterminación informativa, hay cosas que yo no puedo pedir, sí aparezco como propietario de una finca en el registro público yo no puedo pedir por autodeterminación informativa que borren ese dato, que aparece un plano catastrado de esa finca y que dice exactamente que figura tiene, yo no puedo pedir por autodeterminación informativa que quiten el plano, que en registro civil aparece que soy divorciado de mi octavo matrimonio y quiero entrar como postulante a una buena candidata a matrimonio y quiero entrar como un joven casto, no puedo ir al registro civil a que me quiten ese dato. Todo lo contrario lo más inteligente que pueden hacer los padres es ir al registro civil a ver quién soy, o si me avergüenzo de ser abogado no pueden quitar de todos los registros y de todos los archivos mi profesión, máxime si la quiero ejercer.

Entonces la autodeterminación informativa no llega a eso, hay una franja para autodeterminación informativa y es muy importante entender esto. Porque hay un dato que es público y el dato público pertenece al derecho de la información, a la libertad de buscar, de difundir los datos, de comunicarlos de recibirlos y esto no puede ser objeto de ningún control y creo yo que de ninguna seguridad.

Lo que habría allí es un derecho a la integridad, la exactitud, o la calidad de la información.

Si ustedes ponen Federico Malavassi en Internet van a encontrar cosas muy bonitas, muy creativas, muy interesantes, y otras que no le interesan a nadie acerca de Federico Malavassi.

Yo tendría el derecho de corregir esa información, pero no es una información que esté en manos de alguien responsable, se maneja de manera anónima en Internet y posiblemente si ponen imágenes de Federico Malavassi verán que en un blog que se llama "manda huevo", no digo como se llama la otra "cara de no se que…" se imaginarán aparezco manejando una marioneta que tiene la cara de otro diputado. Bueno eso es una imagen que no es cierta, que es reconstruida a modo de caricatura pero es una injuria gráfica y yo no tengo ningún control sobre eso, es más para la salud mental me rió y no me debería importar.

Dichosamente hay otro ámbito de personas, las empresas que manejan la información para cosas serias, y es el tema de las centrales de datos y en este caso voy a hablar de una que conozco, yo soy representante de Datum, asesoro a esta empresa en materia de derecho constitucional. Lo que sucede es que no existe un marco de derecho normativo, solo hay algunas normas de derechos de personalidad de la imagen en el código civil, hay unas normas en el código penal, hay unas normas en el derecho constitucional que son construcciones de la Sala Constitucional basadas o en sus propios antecedentes o en la incorporación del derecho internacional de los derechos humanos ligadas al marco constitucional que deben de proteger.

La Sala Constitucional no tiene una discusión pública como sí la Asamblea Legislativa de este marco normativo, más bien es en la intimidad donde la Sala delibera y algunas veces con magistrados suplentes que aleatoriamente estarán ahí. Por ejemplo incorpora un derecho interesante que si no me equivoco es de una transferencia tecnológica vía de Chile y Alemania que es el derecho al olvido y se estima que cuando una persona ha sido un mal deudor después de un tiempo tiene derecho a que se olvide eso para que pueda- dicen algunos hacer su vida.

La primera vez que lo puso todos los que querían ser olvidados estaban felices, los que querían que les condonaran el crédito de FODESAF, querían ser olvidados y por supuesto corran las centrales a borrar datos de cierta edad sin ningún tipo de precisión jurídica, cuánto tiempo se da cuatro años después de la sentencia. Luego se les demostró que habían créditos que no estaban prescritos que estaban en cobro judicial y que la sentencia podría haberse dictado hace ya 8 o 9 años, pero que si el abogado es diligente y mantiene el cobro de intereses, el crédito estaría vivo, entonces la Sala empezó a no saber cómo sacar las manos y los pies de ese muñeco de cera, que desdibujó ese derecho al olvido que al principio tenía tan claro.

En algún caso solicitó que se quitara de Datum la fotografía de alguna persona, por el trabajo de esa persona requería un cierto grado de intimidad, pero en otros casos no va haber problema porque la fotografía de una persona esté allí. Esto no lo digo para molestar a la Sala Constitucional sino cuán difícil es proyectar un marco de protección a la privacidad, a la autodeterminación informativa cuando estamos ante una realidad que cambia.

Ahora que es lo que sucede con estas centrales de datos de riesgo básicamente porque centrales de datos tenemos casi todos nosotros. Cuando se comienza a hacer directorios y cookies tiene un banco de los procesos que más usa, entonces pone una "C" y le aparece Carlos, son archivos temporales y son pequeñas centrales de datos donde tiene ciertas direcciones de Internet de gente que le ha escrito o que le ha enviado alguna información y ahora la gente está muy celosa de que ese correo no es público, de que lo utilizo para alguna cosa y que le están enviando información no autorizada.

¿Cuánta responsabilidad se tiene con los archivos temporales? ¿Cuánta responsabilidad tiene un profesor? Si por ejemplo en la Universidad de Costa Rica se pasa la lista de discapacitados a una persona porque quiere convocarlos a una asociación y tal vez ofrecerles un producto bien interesante y claro a la persona que está en archivo le parece lo más natural pasa los datos violentando todos los derechos de esas personas a que no se sepa su situación o su estado sea permanente o sea temporal.

Se llevaba la base de datos en una llave, en un disquete en lo que se use y el otro puede utilizar esa información para otras cosas. Les llega la invitación a formar parte de la asociación discapacitados para el mañana cualquier cosa y alguien se siente muy ofendido ¿quién es él y por qué me tiene en esa lista? Una cosa que parecía algo inofensivo.

Datos públicos y publicables

Hay algunas compañías que se han dedicado a recopilar datos públicos y publicables para ayudar a otro sistema el de intermediación financiera. Este es un sistema público no estatal, -que algunos confunden con la banca pero va más allá- sencillamente se descubrió la manera en que los ahorros temporales, los superávit de muchas personas, puedan servir de buchacas para prestarle dinero a otras personas en un determinado plazo.

Incluso las cuentas corrientes, recibimos el salario dejamos unos 10 000 colones en la cuenta corriente durante 10 o 15 días y el banco colecta todo ese dinero de muchas personas y le puede prestar un millón de colones a otra persona a 10 años plazo, a través de una información, de una articulación de conocimientos, que permite saber más o menos con cuánto cuenta. Entonces el sistema de intermediación financiera lo que está usando es el dinero de todos nosotros, el dinero de la sociedad.

Todos nosotros tenemos el derecho de que ese dinero se preste de la mejor manera con la mayor seguridad e incluso, los mismos deudores, tienen derecho a que el costo del dinero sea el más bajo posible, porque si yo soy buena paga, por qué me van a poner el mismo interés que a la persona que es un crédito riesgoso. Ahora si se tratara por ejemplo de la doble condición de crédito que se da una entidad pública, pongamos un banco estatal, todavía los cuidados deben ser más grandes.

Lo que se ha determinado es que debemos utilizar las herramientas de información, para tener así la información de las personas, me contaba un colega que cuando el Banco Nacional le aprobó -hará unos 30 años- el crédito para la casa ya él la tenía construida desde hacía mucho tiempo y ustedes habrán oído muchas anécdotas de este tipo.

Lo que permite el manejo de información de esto que llamamos realidad virtual, pero que a veces no es tan virtual, es precisamente tener acceso a esa información y a los datos que son colectables de una persona o a los datos que se puede tener acceso a través de alguna autorización o a través de alguna manera legítima de compartir información, eso es lo que hace en este caso la empresa a la que yo asesoro. Colecta datos del Servicio Civil, datos del registro Público, datos de la Caja Costarricense del Seguro Social y datos relativos a la identidad de una persona y los tiene en una base con las mayores providencias de seguridad.

Una de las disposiciones de seguridad es que no puede ser consultado sin que no quedara registro de quién las consulta y otra de ellas es que quienes consultan son un club privado bancos, determinadas entidades o determinados profesionales, a través de una suscripción y a través de una autorización y queda registrado exactamente quién hizo la consulta y la hora en la que hizo.

Esto permitió hace poco -con mucho dolor para todos- que una agencia pública la DIS, hizo unas consultas y permitió saber quiénes eran las personas que estaban haciendo las consultas de otras personas. Bueno me parece que esto es seguro, se trata no sólo de datos publicables sino de datos cuyo uso queda registrado. Es el caso de los Magistrados se sintieron medio complicados con la información que dieron y se les llevó sus récords, además quienes los habían consultado, les hizo mucha gracia saber quiénes habían consultado su archivo y además entendieron el sistema.

No todas las compañías de protección de riesgo de créditos son iguales, ustedes recordarán que en la avenida primera había una cosa que se llamaba protectora de crédito, creo que eso es como para llevar a un museo, eso son unos tarjetones que se manejan entre unos comercios y otros, hay otras compañías que sencillamente meten la información.

La sala constitucional

En Datum es casi una religión de la entidad que sus archivos no puedan ser vistos por cualquiera, que el ingreso físico a la compañía sea totalmente limitado y que quede registro de quién uso

la información, pero en algunos momentos ha tenido reprimendas de la Sala Constitucional. En derecho nos enseñan que la jurisprudencia es una forma de derecho no escrita, tendemos a confundirlo con las sentencias, pero las sentencias no son la jurisprudencia. La jurisprudencia es la doctrina que se deriva de los fallos reiterados. Cuando un tribunal tiene fallos reiterados, es decir en la misma línea, puede uno escoger 10, 8, 4 y son reiterados ahí hay jurisprudencia, es la doctrina que se deriva siempre del fallo de los mismos.

Pero la Sala Constitucional en muchísimos aspectos no tiene jurisprudencia; en esta materia ha intentado legislar con la ausencia de un marco normativo, ha ido decantando a hachazos una doctrina, y eso quiere decir que un día permite la foto otro día no permite la foto, un día dice que el derecho de olvido es de 4 años, otro día cambia el concepto, en otra ocasión comete la imprudencia o el error de condenar a la compañía por un dato que aparece en el registro público, por un dato que aparece en los propios índices de los tribunales de justicia.

Cualquiera dice que esa compañía está muy expuesta al litigio, pero no para la cantidad de información que tiene, para el uso que se le da a esa información estamos muy bien, porque siempre se trata de ajustar a la última resolución de la Sala. Tanto que una vez dijo que el dato de determinada persona no se podía enseñar, que se borrara. Pero si después la persona quiere volver a integrarse, y un banco consulta Datum en donde el archivo no está disponible, el banco le dice, tráigame una constancia de que usted no le debe al HSBC, al City, al Banco Nacional, y una constancia de que no tiene hipoteca y de cuáles son sus participaciones en sociedades porque necesitan reconstruir un récord que no tienen. Entonces alguna gente llega y dice miré reincorpóreme de una vez a la base de datos y que se le puede decir a una persona que ha obligado que le borre todos sus archivos, tengo que ir a cada oficina jurídica para ver sí hay algo contra esta persona, tengo que ir a buscar todos los datos del registro civil y del registro público, los que puede tener la CCSS de esta persona, cuánto puede costar esa reconstrucción dentro de esa autodeterminación informativa porque un día quiere ponerse y

otro día quiere quitarse. Lo mejor es que resuelva ella misma sus problemas crediticios, que asuma sus problemas.

Mi tesis jurídica es que una persona no tiene derecho de que la saquen de la base de datos, si los datos son públicos y están legítimamente colectados, sin embargo, la Sala también ha sido errática en este tema. Todos debemos pensar cuáles son los fines y entender que hay unos derechos que hay que armonizar, el derecho de la libertad de exclusión y el de la información por un lado y el derecho de la libertad y del derecho de la privacidad en el ámbito que pueda existir en la red y el de la responsabilidad del uso de esa información en la red.

Estamos en la era de la tecnología y la globalización y esto es imparable, hace muchos años había leído un libro de Marshall Maclujan de la comprensión de los medios de comunicación como extensiones del hombre, lo escribió en 1964, aquí habla no de la electrónica sino de la electricidad que nos había acercado tanto que lo que creaba era una aldea global, ahí están todos los términos que usamos en la actualidad de la globalización, a pesar de que es un tema de comunicaciones. Tanto que algunos autores dicen que la primera etapa fue la era la de la agricultura, la segunda la era industrial y estamos viviendo la tercera, la era de las infocomunicaciones.

Bueno tenemos que aprender conductas y entre esas conductas aprender a guardar la privacidad. La realidad es que ahora trabajamos en redes, nos enviamos los trabajos en pequeñas redes, los profesores ya no piden impresiones de los trabajos sino envíelo por el correo electrónico o póngalo en una llave, hagan trabajos en grupos por lo que la información personal de ellos forman pequeñas bases de datos.

La *Aceptio Veritatis* en el código penal dice que se salva de cometer injuria o cualquier delito para el honor, quién no tenía el animus de injuriar, de difamar o de calumniar y que además había un interés público actual. Y que es interés público actual, ¿el trabajo es de interés público? En cuestiones de vencidad sin duda es de interés público saber quiénes son los vecinos, sí son depredadores sexuales. Sin embargo, lo importante aquí es resguardar tres principios: que el dato sea veraz, exacto y actual.

Finalmente a modo de reflexión yo me pregunto por qué después de que hemos gastado un dineral en el juicio de la Caja Fishel o en algunos de esos juicios, por qué cuando condenen a estas personas no podemos tener acceso a esos datos. Es que acaso no tenemos derecho a saber si estas personas son o no condenadas. Ahí les dejo esa inquietud.

Redes sociales y privacidad

Francia Alfaro Calvo

Las redes sociales de Internet cosntituyen una herramienta escencial en el trabajo de usos estratégicos de TIC y redes de aprendizaje. Las redes sociales tienen hoy dia un increíble auge, son una de los espacios en los que las personas exponen con mayor frecuencia sus datos personales y por ello representan un reto en el tema de privacidad en la red.

¿Por qué la pérdida de privacidad?

Primero voy a empezar por preguntarles ¿por qué perdemos la privacidad en las redes sociales?

El primer problema con el que topamos en las redes sociales, es que contamos con una socialización presencial mas no con una virtual. En nuestro crecimiento alguien se encargó de decirnos: ”Eso no se dice” “eso no se hace”; alguien nos pellizcó para advertirnos cuando decíamos o hacíamos algo fuera de lo esperado. De esta forma nos fueron moldeando nuestras actitudes. En línea no existe este homólogo pues no hay quién nos diga eso se publica, eso no se publica, comunique esto, esto otro no, esa foto no la suba. Entonces hay una ausencia de esa figura de modelaje virtual.

Esto nos lleva a asumir unas conductas de riesgo en línea que no son identificadas como tales, vivo ejemplo de ello es el *spam*, o correo basura. Importante resaltar el nombre tan inocente que tiene el correo basura, a todas las personas que usan correo electrónico le llega correo basura, pero ¿qué es la basura en nuestras vidas?, es algo que estorba y que una hace a un lado y entonces deja de tener implicaciones de mayor riesgo. Pero el correo *spam* nos llega porque nuestra información pesronal está siendo filtrada, alguien conoce nuestros intereses, porque alguien conoce lo que escribimos en nuestros correos.

Deberíamos empezar entonces por cambiar algunos nombres, y darles el nombre que se merecen, en este caso podríamos nombrar el correo basura como raptores de información o perseguidores de consumo, algo que a los usuarios les alerte de lo que esta pasando realmente con su información.

Lo gratuito como ilusión

Las reglas de socialización virtual, las determinan las grandes compañías, no los usuarios. Pasa que las herramientas son identificadas como "neutrales" pero las herramientas virtuales son creadas por personas, y esas personas pertenecen a empresas y esas empresas tienen intereses concretos. De esta forma no es que se nos da espacio a los usuarios para subir fotos e información de manera gratuita porque sí, ese espacio lo obtenemos, porque nuestra información es una mercancía. Más son las redes las que deberían pagarnos por subir esa información.

¿A quién no le gusta ser popular?

Existe una necesidad de ser parte de, ¿cuánto sufrimos en la adolescencia por la popularidad?, por ser más popular. Esto se explica en la recompensa de la popularidad, ser popular significa finalmente ser querido, tener atención, ganar favores, privilecios etc.

La popularidad es otro de los grandes temas en las redes sociales, en las cuales ésta actúa como premio y por tanto como reforzador ya que entre más información comparte, más "popularidad" se gana.

En otras palabras la popularidad se vuelve un acelerador de la entrega de la información. Por tanto agregar al perfil de la red social más personas implican automáticamente volverse más popular ya que el número de "amigos" se incrementa y es visible para todas las personas de dicha red. Es como si pudiéramos caminar con un rótulo que indica cuantas personas conocemos.

En este mismo sentido "subir" o agregar más información personal, más fotos también recibe una recompensa, ya que más personas interactúan con nosotros. La entrega de información por tanto repercute en sentirse atendido, querido, observado, entre otros.

La ilusión del servicio gratuito, lleva a considerar al usuario que colocar más datos, tener un perfil con una plantillas que tenga animaciones, estrellitas que se iluminan, subir más fotos, etc no le implican un gasto de dinero extra por lo que muchas personas entran en un frenesí de ganar 1000 amigos, lo cual es un poco dudoso porque si pensamos en quienes son en realidad nuestros amigos probablemente no lleguen a 1000.

Un nuevo problema que genera esta situación es que las y los usuarios al acostumbrarse a obtener un servicio "gratuito" no se concientizan de la necesidad de pagar por servicios seguros que resguarden su información y en los que se puedan vincular más libremente.

Identidad virtual

Las personas cuando entran a espacios virtuales -como en redes o *chats*- adquieren figuras que los representan. La escala de complejidad es diferente según el espacio, por ejemplo en los *chats* las personas usan *nick* que es un nombre que los identifica posiblemente inlcuso puede ser un seudónimo. En otros espacios como videojuegos en líena se crea un avatar que es una personalización de lo que quisiera ser dentro del juego.

Dentro de las redes sociales creamos un perfil y publicamos una imagen que nos represente, ésta puede ser una fotografía u otro tipo de imagen que no necesariamente concuerda con nuestro aspecto físico, sitaución sobre la cual no existe ningún control que confirme

la veracidad de estas identidades. Esta identidad nos plantea dos riesgos de privacidad, por un lado tenemos a los niños y niñas expuestos a pedófilos que ocultando su verdadera identidad buscan información de sus víctimas que les puedan ser útiles a sus objetivos. Por otra parte el perfil suele dar a las y los usuarios una falsa sensación de anonimato.

Esto último se contradice con nuestra percepción del peligro en el mundo presencial, y aquí cabe resaltar que esta diferenciación entre ambos mundos -virtual y real- la hacemos los que no pertenecemos a generación de los nativos de interent. Estos últimos crecieron con estos dos mundos en constante integración.

En "nuestro" mundo presencial, si se nos acercara un desconocido a solicitarnos datos sobre dónde vivimos y nos solicitara que le enseñemos fotografías de nuestra familia y amigos pensaríamos que "algo anda mal" que esta persona intenta "hacernos algo malo" sin embargo, en la virtualidad las personas no necesariamente crean perfiles privados para proteger su información. Cuando estamos en la red, debemos pensarnos frente a un auditorio (integrado por las personas que hemos aceptado o buscado como amigos) y que cada vez que publicamos algo es como si lo dijéramos en vos alta frente a éste auditorio.

Existe una red que se llama Shared confesión, es una red donde la gente entra y publica un gran secreto, por ejemplo una infidelidad. Hay una confianza en que el sistema funciona bien, y que lo que digan no traerá consecuencias directas.

Los riesgos

Condiciones de uso poco amigables

Hay una confianza "per se" en la red, se los voy a demostrar ¿Quiénes de ustedes están en una red social, Facebook, Hi5? Ahora con total sinceridad ¿quienes leyeron las condiciones de uso antes de entrar a la red,? verdad que todo el mundo dijo "él porque trabaja en el tema de seguridad", pero sí él no hubiera tenido esa formación, esa vocación, a todo el mundo le hubiera parecido rara su conducta.

Lo que se tiende a pensar es que "leer condiciones de uso es de gente rara". Pero es raro llenar la casa de alambres de navaja, no es raro ponerle alarmas a los carros, tener miles de candados, nada de eso es raro, pero leer condiciones de uso es raro y saber qué aceptamos cuando entramos en redes sociales en Internet sí es raro.

¿Ven la disociación que hay entre lo que nosotros aún llamamos mundo presencial con el mundo virtual?

La información se vuelve una mercancía, se está incrementando el número de mujeres en las redes y a su vez hay un mayor número de adolescentes en algunas como Hi5. Con estos dos datos podemos hacernos la siguiente pregunta: ¿existe alguna alerta de esos peligros para estas dos poblaciones?

Cuando una joven sube una fotografía suya en ropa interior, el mismo día, en la misma hora después de la subida, puede ser distribuida por diferentes partes del mundo, son que pueda volver a recuperar todas las copias que se han hecho a su fotografías. Hay entonces una violentación a los derechos de integridad de las personas, pero nadie nos advierte, no existen alertas para advertir a los adolescentes de que corren éstos peligros.

Hay como una noción heredada de que confiar datos es bueno, quizá porque está ligado a la idea de que se recibirá algo a cambio un trabajo, un servicio, etc.

Hace poco en el encuentro preparatorio del foro de "Gobernanza en Internet" en Brasil, una de las personas en la mesa de privacidad se refería a lo alarmante que era Costa Rica por tener el padrón electoral en línea, pues sí, ahí esta nuestro padrón cualquiera lo puede bajar, indica nuestra cédula, fácilmente se puede ubicar quién es nuestra familia, donde vivimos y bueno seguimos con toda esta información ahí, cualquier persona de otro país también la puede bajar. Y si hacemos esta comparación con la redes ya no nos parecen tan graves, requerimos identificar que nuestra información es valiosa, que es peligrosa que sea pública y que requerimos de mecanismos para protegerla.

¿Cuáles son las personas que corren mayor riesgo en las redes? Las personas menores de edad, personas con baja escolaridad, y personas con problemas cognitivos. Y estas persona tienen derecho a saber qué puede suceder con su información, pero éstas amenazas deben ofrecerse con las mismas condiciones de software amigable que las redes sociales en Internet.

No es suficiente ofrecer las condiciones de uso en un documento enorme, en un lenguaje que no es de fácil lectura para poblaciones de bajos niveles educativos. Se requieren *pop ups* de lenguajes sencillo que nos indique los riesgo de subir nuestras imágenes no que diga en las condiciones de uso -por ejemplo en las de Hi5-"usted concede automáticamente a HI5, asegura y garantiza que usted tiene el derecho a conceder una licencia irrevocable, sujetamente no exclusiva, mundial, pagada, para reproducir, mostrar públicamente, interpretar, incluyendo medios digitales para realizar o para ver contenidos de la obra derivada o incorporar el contenido en otras obras, etc."(www.hi5.com, 2009).

Retos

Se requiere crear mecanismos para denunciar y procesar legalmente en nuestro país casos de tratantes y/o explotadores sexuales que detectemos en las redes, timadores, impostores de identidad.

Se requiere también crear programas preventivos para el uso de redes en centros educativos.

Control de daños con la generación de telefonía móvil. Todo esto es en redes imagínense que yo tengo un teléfono en un colegio que ya no es -se acuerdan cuando a uno lo samuelaban en el colegio- ahora es samueleo con la tecnología entonces yo puedo irme a un baño y no sólo ver, sino que puedo sacar fotos, con esta nueva generación de telefonía móvil, aún no estamos tomando en cuenta todas estas cosas.

Incluir programas de usos de redes y de Internet en los programas de alfabetización, no basta que hagamos programas de alfabetización digital para que la gente se meta a la red, sin decirle lo que sucede, lo que puede pasar.

Esto es un tema que debe incluirse en la normativa presente.

Adolescencia y TIC en Costa Rica: nuevas oportunidades, nuevos desafíos

Milena Grillo R.
Walter Esquivel G.

"Para el niño y la niña de hoy, Internet es un espacio de aprendizaje de alfabetización integral, donde no sólo se produce y se comunica en lenguajes multimedia, sino que además se debe saber navegar de una manera crítica entre la sobreabundancia de datos e informaciones que han sido originados con distintos objetivos comunicativos.

Este ciudadano digital requiere de destrezas fundamentales para saber verificar e identificar cuál es la información que le es útil para su desarrollo personal."

Unicef, 2007

La Cumbre Mundial sobre la Sociedad de la Información (Túnez 2005) concluye que las TIC son un instrumento eficaz para promover la paz, la seguridad y la estabilidad, así como para propiciar la democracia, la cohesión social, el buen gobierno y el imperio de la ley en los planos regional, nacional e internacional. De acuerdo con Perez (2008) diferentes autores han puesto de relieve el papel de las TIC en la estructuración de la identidad, la integración social y las representaciones acerca del mundo, desempeñando un lugar relevante en el proceso de socialización de las nuevas generaciones

y ofreciéndoles -juntamente con otros agentes socializadores- estructuras de pensamiento, interacción y acción (Buckingham, 1993; Barker, 1997; Charlton y Neumann-Braun, 1990, Schell, Stolzenburg y Theunert, 1999 o Döring, 2003; citados).

Lo anterior cobra especial relevancia desde el estudio del desarrollo adolescente donde claramente se reconoce la influencia que ejercn las tareas sociales en este momento del ciclo vital, para la definición de la identidad, desde una aspiración de inclusión social. Al respeto Döring (2003) es enfatico en señalar como el auto-concepto, las habilidades sociales o el apoyo social percibido, resultan de gran significación en la comprensión del uso de las TIC que hace o deja de hacer esta población.

Para el caso de Costa Rica, existe preocupación por la acelerada incorporación de sus nuevas generaciones en la Sociedad de la Información y el Conocimiento (SIC) y el efecto que esto puede tener en la formación de su identidad, en términos de valores, aspiraciones y formas de relacionamiento social. Lo anterior por cuanto el uso que hacen de las TIC implica para esta población, una amplia gama de oportunidades --comunicación, desarrollo de la identidad, participación ciudadana, aprendizaje, educación e inserción en el mundo productivo --, pero también de riesgos --tipos de contenido asociados con la explotación sexual comercial y no comercial; la apología de la violencia como medio para resolver conflictos; el racismo y la homofobia; la amenaza a la privacidad o a la propiedad; y la exposición a una comercialización indiscriminada (Livingstone, 2003).

Estas oportunidades o riesgos se entienden asociados a conocimientos y conductas que favorecen, ya sea el uso seguro y responsable o bien el uso irresponsable y riesgoso de las TIC, en la niñez y adolescencia; así como a las medidas que tomen o dejen de tomar sus sociedades de pertenencia, para promover lo primero y prevenir lo segundo.

En este sentido, los hallazgos de una serie de estudios desarrollados por Paniamor entre el 2008 y el 2010, permiten concluir que en Costa Rica, la relación adolescencia, ciberespacio y violencia se percibe asociada a un conjunto comportamientos de riesgo identificados en

los propios adolescentes; sumado a la existencia de factores estructurales que incrementan los riesgos. Estos últimos se ubican en dos dimensiones: aquellos propios del ciberespacio y aquellos presentes en el entorno institucional y social en que se da la interacción.

Una mirada sobre los principales hallazgos de los estudios

Como fuentes propias que sirven de sustento a los siguientes planteamientos se tienen cuatro estudios en el periodo 2008-2010, en el marco de alianzas estratégicas con actores relevantes para el campo de interés. Estos son los siguientes:

- 2008: Estudio. "Uso de Tecnologías de Comunicación e Información en Jóvenes de 12 a 18 años del Gran Área Metropolitana", Fundación Paniamor/Save the Children Suecia (SCS)/ Instituto de Investigaciones Psicológicas de la Universidad de Costa Rica (IIP-UCR);
- 2009: Estudio: "Expresiones de Violencia Interpersonal y Social en el Ciberespacio, desde la vivencia adolescente: Estado del Arte de la Investigación", Fundación Paniamor/Instituto de Investigación para la Justicia de Argentina/Save the Children Suecia (SCS).
- 2009: Diagnóstico "Identificación y caracterización de los sitios virtuales mayormente frecuentados por personas adolescentes en Costa Rica", Fundación Paniamor/Save the Children Suecia (SCS)/RACSA.
- 2010: Estudio "Conocimientos, Actitudes y Prácticas asociados al uso de Internet en adolescentes. Estudio CAP en colegios de la Gran Área Metropolitana de Costa Rica", Fundación Paniamor/.Save the Children Suecia (SCS)/RACSA.

Los principales hallazgos derivados del análisis integrado de dichos estudios se citan a continuación

- Los y las adolescentes recurren a las TIC con frecuencia mostrándose competentes en su uso, lo cual está influido por su posibilidad de tenencia. No obstante, esta característica no refiere ser una variable diferenciadora en cuanto a prácticas de protección en el ciberespacio; por el contrario, pareciera que

mayores niveles de destreza instrumental asociados a mayores grados de exposición/uso, generan un efecto de exceso de confianza en la población usuaria, provocando la disminución de sus estrategias de protección e incrementando los niveles de vulnerabilidad y riesgo.

- Se identifican similitudes en cuanto a las formas de acceso y tipos de uso entre estudiantes del sistema educativo público y privado, mostrándose en este último caso mayores condiciones de tenencia e intensividad de uso y, en ambos casos, limitado o nulo acompañamiento adulto de calidad.
- En cuanto a medios sobresalen la telefonía celular y el uso de Internet, privilegiando aquellas prácticas relacionadas con la socialización, la comunicación y el entretenimiento, tales como la participación en redes sociales, la mensajería instantánea, la búsqueda y descarga de información y el correo electrónico.

En lo que refiere al uso de Internet se observa una tendencia a optar por sitios que de una u otra manera, garantizan inmediatez y disponibilidad de información, servicios y múltiples elementos de una manera integrada, siendo el atractivo visual y la aceptación del sitio entre sus pares, aspectos igualmente relevantes. En lo particular la motivación adolescente para hacer uso de Internet, aparece asociada a la existencia de recursos y servicios de vanguardia, constituyendo el espacio ideal para mostrarse al mundo de la manera en la que se quiere ser visto(a), e interactuar con otras personas trascendiendo los vínculos primarios presentes en el espacio físico próximo.

Cabe destacar el importante significado emocional que otorgan las personas adolescentes a Internet, en particular para niños, niñas y adolescentes (NNA) con propensión alta o media al uso de esta tecnología.

El uso de Internet con fines educativos o académicos representa la actividad menos importante, en comparación con otras actividades ligadas a la socialización y a la comunicación, Al respecto cabe considerar que si bien hay cientos de adolescentes totalmente inmersos en Internet, esto no significa que estén participando significativamente en lo que a opinión, reflexión y construcción de conocimiento se refiere.

Los conocimientos, actitudes y prácticas incrementan vulnerabilidad conforme más años de uso y horas de exposición se reportan. La población adolescente registra desarrollo de competencias técnicas para el uso de Comunicación Mediada por Computadora (CMC); no así, estrategias para el autocuido y el cuido de las otras personas con quienes interactúan en la red.

Si bien no se detectan mayores diferencias en cuanto a acceso a TIC y particularmente a Internet por parte de homriesgosas mayormente asociadas a uno u otro género. Por ejemplo:

- las mujeres adolescentes aparecen como mas propensas a publicar imágenes personales que imitan la sensualidad y erotismo de la publicidad, y que pueden afectar su imagen social exponiéndolas, además, a las expresiones de violencia identificadas;
- los hombres adolescentes, presentan una mayor tendencia a revelar información personal y explorar material nocivo, ilegal y/o inadecuado para la edad, tal como la pornografía, actividad que cuenta con una cierta aprobación social histórica, en tanto se asocia a la construcción de la masculinidad.

No obstante lo anterior, se evidencia una mayor tendencia por parte de las mujeres adolescentes hacia el uso más seguro y más responsable de éste recurso.

La violencia que experimenta la población adolescente en el ciberespacio no representa un nuevo tipo de violencia, sino un traslado de manifestaciones existentes en su entorno físico al contexto virtual, donde adquiere una dimensión distinta en términos de alcance y potencial de daño.

Se identifican como expresiones de violencia frecuentes en las interacciones virtuales, no necesariamente reconocidas como tales por la población sujeto de los estudios, las siguientes: utilización de personas menores de edad en Pornografía, *Morphing, Grooming,* Solicitación Sexual, *Flaming*, Acoso y *matonaje cibernético*, *Sexting,* exposición a contenido no deseado, *Spamming,* robo y fraude virtual.

Aunque la mayoría de adolescentes afirma haber recibido información sobre estrategias de uso seguro y responsable de las TIC,

y reporta poseer conocimientos al respecto, los estudios muestran que las fuentes utilizadas para obtener esa información tienden a ser informales y poco sistemáticas. Esta situación se refleja en la baja o limitada calidad de los conocimientos que manejan.

A este respecto existe coincidencia con resultados obtenidos por PROSIC en su estudio Brecha Digital en la Educación Secundaria: el caso de los estudiantes costarriceses, publicado en octubre de 2009. Esta fuente señala la tendencia de la población a concentrar el acceso a informacion en fuentes autodidácticas o en contactos con amigos y familiares.

Llama la atención el número de conductas riesgosas identificadas en las interacciones virtuales, lo que se vuelve más preocupante si se considera que:

- en muchos casos son los y las mismas adolescentes quienes están ejerciendo algún tipo de violencia sobre sus pares, y
- se hace evidente una ausencia de acompañamiento adulto o bien, la ineficacia de su intervención posiblemente asociada a su desconocimiento de los usos que las personas menores de edad hacen de la web y en general de las TIC.

Reforzando el anterior anlisis, las fuentes utilizadas coinciden con otros estudios internacionales, en demostrar el carente o nulo acompañamiento que las y los adultos brindan a las personas menores de edad en sus interacciones virtuales, lo cual se evidencia con mayor fuerza entre los grupos con mayor poder adquisitivo.

- Padres y madres tienen poca injerencia sobre este medio, es decir, no son censores pero tampoco asesores en el uso.
- Padres y madres conocen las páginas visitadas por sus hijos e hijas pero se abstienen de comentarles al respecto.
- Adolescentes clasificados como altos usuarios tienen padres y madres que son altos usuarios también, por lo que bien podrían fungir como sus interlocutores en este ambito.

Los niveles de victimización tienden a ser muy variables dependiendo de la situación específica, pero sobresalen aquellos rela-

cionados con la recepción de información no deseada, la alteración de datos de terceras personas e insistencia de desconocidos/as para entrar en contacto. Las actitudes son en general apenas moderadas, evidenciándose algunas disposiciones hacia prácticas de riesgo, en especial en lo que respecta a la agresividad y la violencia en sus comunicaciones.

Si bien existen condiciones en la Web que potencian la manifestación de la violencia en sus distintas expresiones, el problema parece no radicar en la herramienta propiamente sino en el uso que las personas adultas y las personas menores de edad hacen de ella.

A pesar de lo anterior, el análisis de las prácticas en la red evidencia, en la mayoría de la población considerada en el estudio del 2009, una tendencia responsable en lo que respecta a la toma de posibles riesgos en el uso de Internet. Sin embargo una tercera parte de esta población reporta una conducta de menor seguridad.

Algunos datos concretos para reflexionar

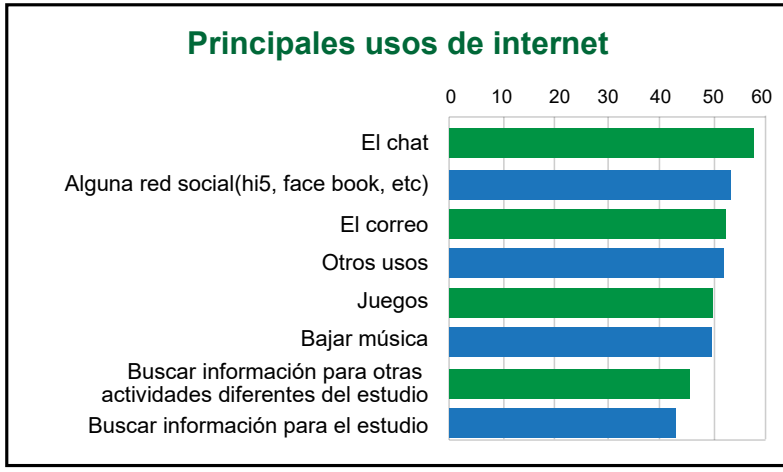
El Estudio "Conocimientos, Actitudes y Prácticas asociados al uso de Internet en adolescentes. de colegios de la Gran Área Metropolitana de Costa Rica" (2010), desarrollado con 402 adolescentes hombres y mujeres, estudiantes de centros públicos y privados; desde su abordaje cualitativo y cuantitativo permite extraer algunos datos que llaman a la sociedad costarricense no sólo a la reflexión, sino a la construcción pronta e inteligente de respuestas. Este estudio con un 5% de margen de error, empleó un instrumento con una escala de conocimientos, una de actitudes subdividida en seis secciones y una batería de preguntas cerradas acerca de las prácticas en el uso de Internet de esta población. Entre estos datos cabe resaltar los siguientes:

En cuanto a usos

- 21% de la población encuestada utiliza la red 20 o más horas a la semana. La mayoría de las personas adolescentes entrevistadas tienen varios años de utilizar Internet. 77,7% cuenta con conexión en el hogar. El 64,4% de los y las adolescentes que

estudian en colegios públicos poseen conexión a Internet en su hogar, mientras que entre quienes estudian en colegios privados esta proporción llega al 91,4%.

- La búsqueda de información para el estudio representa la actividad menos importante. El uso principal de la red tiende a concentrarse en procesos de comunicación social, tales como el chat, las redes sociales o el correo.



Los conocimientos sobre uso seguro y responsable parecen ser menores en personas con alto uso de Internet. Tanto las situaciones de riesgo como las actitudes negativas tienden a incrementarse conforme aumenta el uso de la red. La situación es más crítica entre las personas con conexión en el hogar, con más años de uso y con más horas de conexión por semana. Esto podría estar evidenciando, no tanto una falta de información, como el desarrollo de actitudes y hábitos en función del uso prolongado de la red, que podrían verse reforzados ante una baja frecuencia de atribución de resposabilidades como resultado de la acción negativa.

Tanto los conocimientos como las actitudes y las prácticas resultan generalmente mejores entre las mujeres en comparación con los hombres.

En cuanto a conocimientos

Las principales fuentes de informacion sobre uso seguro y responsable son amistades y familiares. El acceso a fuentes más sistemáticas como programas educativos, charlas, cursos o folletos tiende a ser relativamente baja (28,5%). Posiblemente esto ayude a explicar el alto interés que muestran por conocer más sobre el tema y el bajo nivel observado en los conocimientos.

62.5% cree que deben tomarse riesgos en el ciberespacio para dominarlo. El rendimiento en la escala de conocimientos es pobre (promedio de 46,4 en la escala de 0 a 100), evidenciándose, además de la creencia en tomar riesgos innecesarios, algún exceso en el uso de la red en detrimento de otras actividades importantes, suministro inconveniente de información, manejo inseguro de posibles acosos, y en especial la reacción e inclusive la participación en comunicaciones agresivas.

Tanto las ideas que sustentan un uso no responsable como aquellas que facilitan un uso inseguro o riesgoso se encuentran bien afianzadas, lo cual dificultaría cualquier esfuerzo de modificación de actitudes y prácticas.

En cuanto a actitudes

Existe una predisposicion para utilizar poco la Internet para el estudio (16,9%) en contraste con la de Internet para la socialización (51,6%). Los promedios en las diferentes subescalas tienden a ser apenas moderados o bajos. Se evidencia, una actitud ambivalente con respecto al efecto de la red sobre las relaciones sociales y hacia el uso de información personal.

61,7% no muestra disposición a controlar el tiempo dedicado a Internet. El poco control sobre el tiempo dedicado a la red provoca la sensación de que se han reducido las posibilidades de realizar otro tipo de actividades alternativas y que el uso de Internet genera a menudo conflictos con sus adultos encargados.

También existe una cierta predisposición a la participación en comunicaciones agresivas. Las actitudes son más positivas en cuanto al

rechazo del acoso, de la pornografía y de las interaciones sexuales virtuales.

Existe la percepcion de que se es más respetable entre más amigos y amigas se tengan en las redes sociales. En lo que respecta a las relaciones sociales por Internet, es importante resaltar que existen contradicciones interesantes en las actitudes de esta dimensión, puesto que por una parte, la mayoría de las personas entrevistadas rechaza la discriminación social por el no uso de Internet, pero al mismo tiempo muestra un respeto diferenciado según la cantidad de amistades que se tenga en las redes sociales.

Priva la sensación de que las personas son menos tímidas en Internet y que los problemas personales se resuelvan mejor en Internet que frente a frente. Mientras la mayoría considera que es posible lograr una amistad íntima con aguien aunque no utilice Internet, al mismo tiempo se considera que las personas son menos tímidas en la red y que los problemas se resuelven más fácilmente en Internet.

Se reconocen riesgos asociados al manejo de la imagen y la informacion personal en las redes sociales. Se reconoce que datos y fotos de una persona pueden ser fácilmente alterados en una red social y que las personas tienden a mentir en sus perfiles, pero por otro lado, en contraposición, se desconfía de quien no suministra fotos.

70,3% reconoce no evitar la participación en chats con gente agresiva. Existe cierta predisposición a participar activamente en comunicaciones agresivas. La población no muestra una tendencia a evitar este tipo de relaciones y, por el contrario, cerca de una tercera parte registra tendencia a insultar a otras personas en Internet y casi la mitad a participar en chismes a través de la red.

Se evidencia un interés o al menos una curiosidad por páginas con contenido violento o desagradable. Dos terceras partes aceptan tener curiosidad por páginas con contenido violento, cerca de la mitad no cierra este tipo de páginas cuando ingresa a ellas por error, y casi tres cuartas partes no puede evitar el curiosear páginas con contenidos desagradables.

74,3% considera poco agradables los contenidos pornográficos en Internet. La mayoría de los y las adolescentes consultados muestra una actitud responsable y protectora con respecto a la pornografía en la red.

82,7% muestra poco o ningún interés en conversaciones sobre intimidades sexuales en Internet. La mayoría de los y las adolescentes consultados también muestra una actitud responsable y protectora con respecto a las interacciones sexuales virtuales.

En cuanto a prácticas

Se identifican niveles altos de victimizacion mediados por Internet. Las proporciones de adolescentes que han sufrido algún tipo de victimización tienden a ser muy altas. Así, por ejemplo, un 70,7% dice haber recibido información no deseada, un 68,7% información falsa de otras personas, un 53,9% insistencia de un/a desconocido/a para entrar en contacto, y un 47,1% ha recibido conversaciones agresivas con ofensas o insultos.

Un 33,9% ha limitado su dedicación al estudio por el uso de Internet y un 28,1% ha reducido el ejercicio físico. Aunque la mayoría de los y las adolescentes afirman tener un buen control sobre el tiempo dedicado a la red, existe un grupo no desdeñable que evidencia una disposición hacia el exceso, en detrimento de actividades importantes como las comidas, el sueño, el ejercicio, las actividades sociales y el estudio.

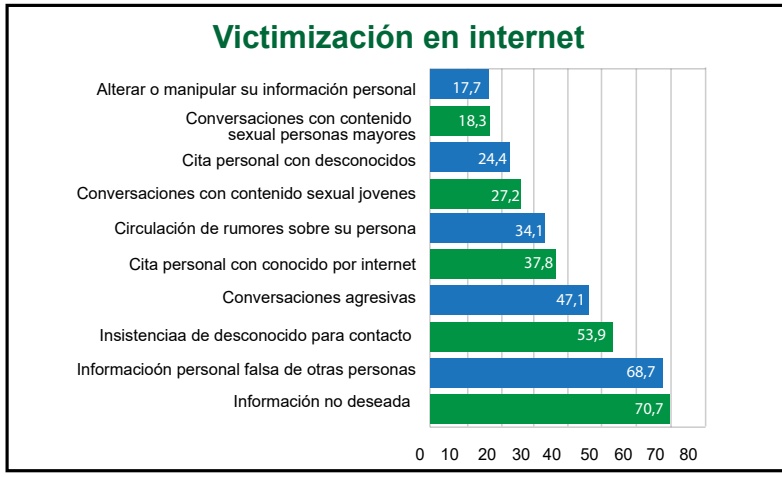
Aunque un 62.5% afirma creer que es necesario tomar riesgos en el ciberespacio, un 85,4% en promedio reporta no tomar nunca ninguno de los riesgos evaluados. La tendencia reportada a tomar riesgos al usar Internet resulta particularmente baja. Así, por ejemplo, priva un cuidado responsable sobre el tipo de información que no debe brindarse en las redes sociales, aunque cerca de una tercera parte acepta haber utilizado información falsa o alterada. No obstante, se observa de nuevo la participación en comunicaciones agresivas.

63.5% reporta nunca aceptar un contacto en Internet con adultos desconocidos. Se evidencia en la mayoría un manejo responsable y protector de las situaciones de posible acoso.

25,1% reconoce haber promovido conversaciones agresivas con ofensas e insultos en Internet. En concordancia con las actitudes favorables hacia la agresividad en Internet, una proporción importante de las personas adolescentes entrevistadas reconoce participar e inclusive promover relaciones agresivas.

30% acepta haber buscado contenidos pornograficos de manera activa y voluntaria. La exposición a contenidos de pornografía resulta relativamente alta, con un importante acceso a este tipo de páginas tanto de manera involuntaria como voluntaria.

Una sintesis de las practicas de riesgo que experimenta la población adolescente en Costa Rica, segun fueron identificadas en el estudio de comentario, se recoge en en el siguiente gráfico.



Hacia la construcción de respuestas ante los desafíos identificados

La preocupación existente en el contexto nacional sobre como responder a los riesgos reales que enfrentan NNA en sus interacciones en el ciberespacio, es compartida universalmente. Dos enfoques de aproximación al problema que han marcado la deliberación internacional, merecen ser traídos a la reflexión nacional como marco referencial para avanzar a la construcción de lo que ha de ser la

respuesta de Costa Rica a los desafíos que la problemática bajo estudio conlleva.

Un primer enfoque, promovido bajo el lema Navega Protegido, sustenta iniciativas que abanderan la imposición de un control externo de los riesgos, a cargo mayoritariamente de las personas adultas. Como expresiones operativas de este enfoque, se reconocen el uso de software de control parental; la creación de sitios controlados para uso exclusivo de niños libres de contenido nocivo y de acceso totalmente restringido a usuarios no previamente autorizados, la fiscalización indiscriminada de las interacciones y las comunicaciones de las personas menores de edad suponiendo una violación a su privacidad, desde un paradigma de situación irregular que considera a NNA como seres vulnerables per se e incapaces de desempeñarse de manera segura y responsable según el momento del ciclo vital en el que se encuentren, como sujetos de derechos y responsabilidades que son.

Al respecto, diversos estudios nacionales e internacionales orientan a pensar que es partir de cambios en conocimientos, actitudes y prácticas de NNA y no desde la limitación del acceso a la información y las relaciones, que se evitará el impacto de los riesgos en ambientes virtuales. Más aún, el enfoque comentado presenta riesgos significativos en cuento al cumplimiento del derecho de NNA a un Uso Seguro y Responsable de las TIC, en tanto deja espacio para decisiones adultocéntricas arbitrarias en cuento a acceso y uso, niega el derecho y la capacidad de NNA de participar significativamente en asuntos que les afecta, limita los esfuerzos de enfrentamiento del Brecha Digital que afecta a población menor de edad en desventaja social y, llevado a un extremo, puede llevar a satanizar la relación de NNA con las TIC como un todo.

Un segundo enfoque, expresado en el lema Navega Seguro, sustenta iniciativas que más bien promueven la corresponsabilidad entre el mundo adulto y la niñez y la adolescencia, para el logro de los fines buscados. Este supuesto parte de reconocer el rol protagónico que por derecho propio y por capacidad suficiente, le corresponde ocupar a la persona menor de edad como sujeto social, en la reflexión, discernimiento y toma de decisiones relacionadas con la propia protección y

la de otras personas frente a los riesgos del Ciberespacio, según sea adecuado para su nivel de desarrollo y madurez.

Por lo demás, Navega Seguro no es omiso en señalar la responsabilidad que recae sobre las familias y otras personas adultas con funciones de formación de NNA, así como sobre los otros garantes del derecho que reivindica, en la creación de condiciones que minimizan los factores y conductas de riesgo, al tiempo que potencian los factores y conductas protectoras, de NNA frente a la violencia en el Ciberspacio. Esto desde el acompañamiento y no desde la imposición; desde la potenciación y no de la limitación; en consistencia con los Principios de Autoridad Parental, Autonomía Progresiva, Rol Supletorio del Estado, Participación Significativa de NNA y No Discriminación propios de la doctrina de los Derechos de la Niñez y la Adolescencia.

La Posición de la Fundación Paniamor

La Fundación Paniamor de Costa Rica, como organización de la sociedad civil con más de veinte años trabajando por el cumplimiento de los derechos de niñas, niños y adolescentes; asume el enfoque Navega Seguro como parámetro rector de todas las iniciativas que la organización desarrolla o llegue a desarrollar en respuesta a los desafíos que conlleva el hacer realidad el derecho de las personas menores de edad a un uso seguro, responsable y productivo de las oportunidades que ofrece la cultura tecnologica. Desde este posicionamiento, Paniamor:

Postula que:

- El uso intenso de TIC por parte de población menor de edad en Costa Rica hace necesario reconocer el ciberespacio como un nuevo ámbito de socialización que requiere ser mediado adecuadamente, con participación significativa de la propia población. Esto con el fin de potenciarlo en todo lo que ofrece de constructivo, así como de neutralizarlo en lo que encierra en términos tanto de factores de riesgo presentes en su contexto, como de comportamientos de riesgo en los que pueda incurrir esta población, por insuficiencia de las competencias esenciales para hacer un uso constructivo de las TIC en función de su crecimiento personal y desu progreso social.

- La mediación que se construya en el país para potenciar la relación de la niñez y la adolescencia en este nuevo espacio de socialización debe tener presente - y enfrentar asertivamente- el hecho comprobado de que el uso inadecuado de estos medios y espacios, conlleva peligros y es terreno fértil para una socialización no constructiva de esta población.
- El uso creativo y productivo de estos mismos medios encierra un potencial extraordinario, aún no aprovechado en el país, para promover los valores inherentes a una cultura de paz en sus nuevas generaciones usuarias de las TIC, así como para movilizar su participación activa en el rechazo de las diversas expresiones de violencia social que atentan contra su propio desarrollo y ponen en peligro la paz y la convivencia democrática de la nación costarricense, como un todo.
- Los actores institucionales y sociales con mandatos relacionados requieren ser sensibilizados y movilizados para que asuman su rol como garantes de tales derechos.

Se compromete a:

- Participar de manera activa en todo esfuerzo nacional, sectorial o institucional que en esencia resulte coincidente con los valores y principios que subyacen del enfoque Navega Seguro, según ha sido planteado.
- Poner la experiencia y los aprendizajes acumulados por la organización en el ambito bajo estudio, a disposición de las autoridades públicas con mandatos relacionados, con el propósito de contribuir de la forma que se estime oportuna, hacia el desarrollo e implementación de políticas públicas y buenas prácticas sectoriales e institucionales orientadas a la protección y defensa de los derechos de NNA en el con texto virtual.

Agradece a:

El Programa de la Sociedad de la Información y el Conocimiento (PROSIC) de la Universidad de Costa Rica por el espacio abierto en esta publicación al tema aqui tratado. Esta consideración adquiere especial relevancia a la luz del pronunciamiento de la

Sala Constitucional, en su sentencia número 10627 del 18 de junio de 2010. En esta sentencia se declara que el acceso a Internet es un derecho fundamental por tratarse de un vehículo indispensable y necesario para que las personas, sin discriminación, devengan en partes legítimas de la Sociedad de la Información y el Conocimiento. Lo anterior, por ende, aplicable al reconocimiento del derecho de cada niña, niño y adolescente:

- por su condición de persona, de acceder y participar en la producción de la información y el conocimiento como bienes públicos que son, indispensables para ejercer esa libertad de pensamiento y de expresión que consagra la Convención Internacional de los Derechos del Niño de las Naciones Unidas y su expresión nacional, el Código de la Niñez y la Adolescencia de Costa Rica, para todas las personas menores de edad que habitan en esta nación; y
- por su condición de persona en proceso de desarrollo, a ejercer tal derecho en un marco de protección especial, asegurado al mayor nivel posible por el Estado con la participación decidida de sus familias y otros actores economicos y sociales con mandatos o responsabilidades relacionadas.
- Hermosa oportunidad, hermoso desafío que convoca a la Academia para ocupar en ello un rol singular.

Bibliografía consultada

Benedikt, M. “Cyberespace: Some proposals”. En M. Benedikt (Ed.) Cyberespace: First steps. Cambridge, MA: The MIT Press, 1991.Bermudez E y Martínez G. (2001) “Los estudios culturales en la era del ciberespacio. Universidad de Zulia, Venezuela. Disponible en: http://convergencia.uaemex.mx/rev26/26pdf/Ciberespacio.pdf.

Castells, Manuel (2002). La Dimension Cultural de Internet. Universitat Oberta de Catalunya. España. Disponibel en http://www.uoc.edu/culturaxxi/esp/articles/castells0502/castells0502.html.

Castells, M. (...) Internet y la sociedad red. Clase inaugural Doctorado de la Sociedad de la Información y el Conocimiento. Universitat

Oberta de Catalunya. España. Disponible en http://www.uoc.es/web/cat/articles/castells/castellsmain1.html.

Castells, Manuel. La era de la información: Economía, sociedad y cultura, vol 1, La sociedad red. Madrid, Alianza, 1999.

Chicos.net, ECPAT y Save de Children (2008) "Chic@s y tecnología: usos y costumbres de niñas, niños y adolescentes en relación a las Tecnologías de la Información y la Comunicación".

ECPAT International (2005) "La violencia contra los niños en el ciberespacio".

International Network Against CyberHate- INACH (2007) "Second INACH Report" Disponible en: http://www.inach.net/content/second-INACH-report.pdf.

Ofcom (2008) "Social Networking: a quantitative and qualitative research report into attitudes, behaviours and use. Disponible en www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/socialnetworking/report.pdf.

Paniamor/IIJ/SCS. (2009) Expresiones de violencia interpersonal y social en el ciberespacio desde la perspectiva adolescente: Estado del Arte.

Paniamor/SCS/RACSA. (2009) Diagnóstico: Identificación y caracterización de los sitios virtuales mayormente frecuentados por personas adolescentes en Costa Rica".

Paniamor/SCS/RACSA. (2010) Estudio Conocimientos, Actitudes y Prácticas asociados al uso de Internet en adolescentes. Estudio CAP en colegios de la Gran Área Metropolitana de Costa Rica.

Peña, M. (2006). La Responsabilidad del Estado en el cumplimiento de los Derechos de la Infancia y la Adolescencia: Responsabilidad Parental versus Autonomía Progresiva del Niño. II Seminario Latinoamericano de la infancia y adolescencia. Universidad Nacional de Rosario, Argentina y Universidad Nacional de Asunción, Paraguay.

Pérez, R. (2008.). Uso de Tecnologías de la Comunicación e Información en Jóvenes de 12 a 18 años del Gran Área Metropolitana.

Instituto de Investigaciones Psicológicas Save the Chidren Suecia-Fundación Paniamor. Costa Rica.

PROSIC (2008) "Hacia la Sociedad de la Información y el Conocimiento en Costa Rica: Informe 2008." San José, C.R.: Universidad de Costa Rica.

Society at Harvard University & The Berkman Center for the intenert (2008) "Emhancing Child Safety & Online technologies: Final Report". Disponible en: http://cyber.law.harvard.edu/research/isttf.

The National Campaing to Prevent Teen and Unplanned Pregnancy & COSMOgirl.com (2008) "SEX AND TECH : Results from a Survey of Teens and Young Adults " Massachussetts. Disponible en: http://www.thenationalcampaign.org/sextech/.

Unicef (2007) "¿Autorregulación?... y más: la protección y defensa de los derechos de la infancia en Internet". Unicef.

Youth Protection Roundtable (2007) "Results of an expert survey on matters of safer Internet and youth protection in Europe." Alemania.

Capítulo 3
Firma digital y ciberseguridad

Los cerrajeros de la sociedad digital

Carlos Melegatti Sarlo

En el mundo físico el tener muchas llaves hace nuestras vidas complicadas, la llave de la puerta de la casa, de la oficina, del carro, entre muchas otras. Cada una con formas y características diferentes, utilizadas todas para atender un objetivo básico y esencial: tener acceso a un recinto u objeto.

En esas condiciones, es normal querer simplificar las cosas y cambiar todas esas llaves por una única, equivalente a una llave maestra, la cual nos permita el acceso universal a cualquier lugar o dispositivo al que estemos autorizados.

En el mundo digital el uso de llaves es un tema aún más complejo. Las personas son clientes de múltiples bancos y usuarios de sus sitios web; muy probablemente también usuarios de varios sistemas informáticos en la empresa donde laboran, clientes de algunos servicios ofrecidos en la Web por las diversas entidades públicas y privadas del país, y para todo eso se necesita una llave, un acceso.

La configuración de las claves de acceso a los múltiples sistemas informáticos a los que ingresamos a diario son variadas, obligando

al usuario a administrar complejos sistemas de codificación que en la mayoría de los casos corresponde a un código de usuario y una palabra clave. Además, existen otros dispositivos de reciente utilización que responden a políticas de seguridad diferentes según cada institución o empresa.

Por ello, no es extraño que la palabra clave que debamos definir cuando utilizamos un sistema informático de una institución especifica se deba formar, según sus políticas, utilizando mayúsculas, minúsculas, números y signos especiales y en otras simplemente los números no sean permitidos, esto por solo mencionar un ejemplo.

Lo anterior evidencia que a medida que continúe el desarrollo de aplicaciones web orientadas al ciudadano, estaremos sometidos a gestionar una mayor cantidad de esquemas de acceso para llevar a cabo los procesos de identificación requeridos en dichos sitios, lo que denota la necesidad de redefinir la forma tradicional de identificación electrónica de usuarios sobre los sistemas computacionales, conocida como autenticación de usuarios, así como la definición de atributos y derechos sobre dichos sistemas.

En el mundo digital, construir una llave maestra que nos permita tener acceso a las variadas funcionalidades de las plataformas tecnológicas en la red, es imprescindible para un correcto desarrollo futuro. Ya no serían necesarios códigos de usuarios y palabras claves diferentes para diferentes aplicaciones informáticas, pues con una llave maestra asociada directamente a la persona - una Identidad Digital - , se podría acceder a los múltiples servicios que se tenga derecho a utilizar en los diferentes sitios web.

La seguridad digital y los secretos

Para tener una llave maestra y acceder cualquier aplicación informática, en particular funcionalidades provistas a través internet; las técnicas y dispositivos empleados deben garantizar una adecuada atención de las amenazas a las que están enfrentadas las tecnologías de información y comunicación en la actualidad, evitando o reduciendo en forma significativa los riesgos inherentes a su uso.

Todo esquema de seguridad digital está soportado en la administración de secretos. El PIN utilizado en los cajeros automáticos para

disponer de fondos de una cuenta es un secreto, la palabra clave o *"password"* es igualmente un secreto. El problema de los secretos es que se exponen.

Exponemos el secreto cuando lo digitamos al tratar de ingresar a cualquier sistema, nuestro secreto se copia en la memoria del computador utilizado, podría viajar a través de la red o podría ser almacenado en algún dispositivo conectado a nuestro equipo. De esa forma, los secretos al ser expuestos pueden ser copiados, siendo ahí donde toman forma una gran cantidad de estrategias computacionales diseñadas para adueñarse de los mismos y con ellos realizar transacciones fraudulentas a nuestro nombre: *Phishing y Keyloggers*, son solo algunas de las técnicas automáticas más conocidos para tal efecto.

Si las técnicas de sustracción automáticas de información no son suficientes para apoderarse de los secretos, suplantar la identidad de un usuario y accesar los sistemas a nombre de éste, existen otras técnicas agrupadas en un concepto denominado "Ingeniería Social", las cuales explotan las debilidades organizacionales o de formación de las personas en cuanto a los cuidados básicos alrededor del manejo de información sensible. En ese sentido, se conoce de casos en que una persona haciéndose pasar por funcionario de una Institución, solicita información vital a un cliente, en donde a través del engaño logra conseguir la información requerida y así sustraer el tal preciado secreto.

Los certificados digitales: "las llaves maestras"

En la Ley Nº 8454 sobre Certificados, Firmas Digitales y Documentos Electrónicos y su respectivo reglamento, se encuentra el marco jurídico para la emisión y distribución de las llaves maestras digitales, los cuales en el lenguaje de la propia Ley se denominan "certificados digitales". Este certificado es un documento electrónico, que se asocia en forma directa con la identidad de una persona física y que es emitido por una Autoridad Certificadora (AC) siguiendo los más altos estándares de seguridad.

Una AC, según la Ley, puede ser cualquier empresa privada o pública que aprueba estrictos controles de calidad y que demuestra

alta capacidad técnica y administrativa para tal efecto. Así, tanto un banco, una institución pública o una empresa privada pueden convertirse en AC y construir las infraestructuras necesarias para emitir y distribuir certificados digitales.

Técnicamente hablando, un certificado digital es un documento electrónico firmado digitalmente por la AC emisora del mismo, en donde la firma digital de la AC da fe que el certificado emitido es efectivamente de quien dice ser. En otras palabras, la AC emite un documento electrónico y da fe que ese documento se asocia en forma única con una persona física (similar a lo que hace el Tribunal Supremo de Elecciones con nuestras cédulas de identidad), siendo este documento electrónico la llave maestra que estamos buscando para ser reconocidos al ingresar a cualquier sitio web.

Un certificado digital firmado no es más que un documento digital codificado, el cual garantiza la autenticidad e integridad del mismo. Dicho documento será alojado posterior a su emisión dentro de una tarjeta con un "chip electrónico", dispositivo que garantizará una protección segura del mismo.

Los retos para emitir y distribuir certificados digitales

Cualquier empresa, privada o pública que cumpla con estrictas normas de seguridad y calidad, puede potencialmente transformarse en una AC y emitir certificados digitales.

Pero, aunque en teoría esto es así, en la práctica tales infraestructuras requieren inversiones millonarias para hacerlas realidad.

La experiencia internacional señala que cuando esas infraestructuras se construyen con un evidente fin de lucro, más que una estrategia país para el desarrollo de la Banca en Línea, el apoyo al desarrollo del Gobierno Digital y la consolidación del Comercio Electrónico, estos certificados son sumamente costosos para el cliente, convirtiéndose en un obstáculo para tales desarrollos. Hay muchos países donde la emisión de un certificado digital tiene un costo entre 50 y 100 dólares anuales, cifra que evidentemente es una barrera de entrada a la masificación de estas tecnologías.

En el Banco Central de Costa Rica, nos dimos a la tarea de definir un modelo de operación para la emisión y distribución de certificados digitales para el sector financiero, el cual tiene como principal objetivo la reutilización de las infraestructuras electrónicas y físicas que dispone actualmente dicho sector. Es así como hemos gestionado la puesta en marcha de una Autoridad Certificadora en el propio Banco Central, apoyada en la infraestructura física y tecnológica existente para cumplir con lo requerido.

Hemos implementado un servicio electrónico para la emisión de certificados digitales utilizando al Sistema Financiero como centros de distribución de los mismos. Este servicio se ampara en la plataforma tecnológica del Sistema Nacional de Pagos Electrónicos (SINPE), infraestructura que actualmente procesa alrededor de 120 mil operaciones diarias, por alrededor de ¢250 mil millones, esquema operativo que tiene ya más de 12 años de operación y sirve para interconectar a todo el sistema financiero nacional.

En concreto, estamos preparando las sucursales de los Bancos para realizar dicha distribución, es decir, un cliente de una Institución Financiera puede presentarse en la plataforma de servicios de su banco y solicitar su certificado digital, en idéntica forma a como en este momento solicita una tarjeta de crédito, de débito, una chequera o cualquier otro instrumento financiero.

Este certificado digital o llave maestra, le permitirá a los clientes bancarios, en primera instancia, ingresar y autenticarse al propio sitio web de dicha entidad, pero por su condición de llave maestra, con el mismo certificado podría acceder y realizar transacciones a cualquier otro sitio web disponible en el país, el cual confié en este certificado digital emitido por el SINPE.

Este esquema de trabajo aprovecha al máximo las instalaciones físicas y electrónicas existentes en el Banco Central, la infraestructura del Sistema Nacional de Pagos, las relaciones electrónicas que se han construido a lo largo de los años con la banca, las propias sucursales bancarias y sus seguros sistemas de operación, entre muchos otros elementos con que cuenta actualmente el país.

Todo lo anterior nos ha permitido construir un sistema de emisión y distribución de certificados digitales, de muy alta calidad y seguridad y a muy bajo costo, lo que esperamos redunde en una masificación significativa de estas tecnologías de seguridad, las cuales aportan robustez al desarrollo de las plataformas empleadas para implementar servicios en el mundo digital.

Sobre los riesgos asociados a la emisión y uso de la firma

Las exigencias sobre la calidad de cualquier proyecto, están determinadas en relación directa con los riesgos inherentes al mismo y de las implicaciones que este producirá en su operación sobre los clientes, las empresas, la sociedad y en general el entorno potencialmente afectado.

Para comprender de mejor forma los riesgos que enfrentamos y los altos requerimientos involucrados en un proyecto como el que nos ocupa, podemos utilizar algunos casos prácticos para denotar a que nos referimos.

Así por ejemplo, en el mundo físico, cuando debemos realizar un trámite particular, en donde nuestra presencia sea necesaria para que, luego de identificarse, proceder a firmar el documento que especifica las características de una transacción: comprar un automóvil o una casa, solicitar una línea telefónica, solicitar un servicio público, en general, lo típico de la firma de un contrato para proceder a recibir un bien o servicio.

En resumen, en el mundo físico luego de identificarnos, procedemos por lo general a firmar sobre un papel, siendo esta firma la que nos compromete jurídicamente, ya que de puño y letra damos fe, aceptando y comprometiéndonos con el trato en cuestión.

Por otra parte, en el mundo digital, contamos con certificados digitales para autenticarnos, lo que es lo mismo que identificarnos electrónicamente y también, firmar digitalmente transacciones que nos comprometen jurídicamente, todo esto sin nuestra presencia física, en un contexto eminentemente digital, todo a través de un sistema. En este escenario es relativamente fácil deducir que los procesos para emitir, distribuir y entregar certificados digitales a las personas deben

responder a los más altos estándares de calidad y seguridad, ya que el entregar un certificado digital incorrectamente, puede potencialmente implicar responsabilidades jurídicas para su legítimo dueño, si este es utilizado indebidamente para suplantar su identidad.

Es así como la existencia de la firma digital permitirá al ciudadano de un sin número de novedosos y muy útiles servicios digitales, pero esta potente tecnología requerirá también de la atención de estrictos cuidados. Para las Autoridades Certificadoras("Los cerrajeros Digitales"), de garantizar la existencia de los mejores procesos y procedimientos para la emisión, distribución y entrega de los certificados digitales al ciudadano, por ello trabajamos esta construcción siguiendo la norma INTE-ISO-21188:2006, norma internacionalmente aceptada y en la cual se especifican las mejores prácticas en esta materia; Para las personas, el mayor cuidado con respecto al resguardo del dispositivo(tarjeta) que contiene nuestro certificado digital, ya que un descuido puede implicar que alguien suplante digitalmente nuestra identidad y realice a nuestro nombre transacciones que puedan comprometernos.

Preparando los sitios web

Estamos claros que la existencia de una llave maestra asociada en forma unívoca a cada persona, que desempeñe el rol de una identidad digital, facilitará en forma significativa la operativa y seguridad de los usuarios al utilizar facilidades disponibles en Internet, solo que esto demanda que las instituciones públicas y privadas que ofrecen servicios digitales, deban preparar sus infraestructuras para permitir a los usuarios autenticarse utilizando esta identidad digital de uso general.

En relación con lo anterior, en Costa Rica el nivel evolutivo de los sistemas que utilizan la red internet presentan grados de desarrollo significativamente diferentes. Los más avanzados son sin duda alguna los sitios transaccionales asociados a la banca. En ellos encontramos una variada cantidad de transacciones disponibles, algunas muy sensibles, como por ejemplo los procesos de movimiento de fondos entre cuentas de clientes, la revisión de estados de cuentas, el pago de los tributos municipales, entre muchos otros.

Para estos sitios, los trabajos de adaptación de sus infraestructuras son relativamente simples, afirmación que se apoya en el hecho de que estas instituciones por años han hecho el trabajo en forma consistente, han logrado sacar a los usuarios de sus sucursales físicas y los han desplazado a utilizar sus sitios web. En este caso, básicamente el trabajo que falta por realizar es permitir que sus clientes puedan ingresar a estos servicios utilizando un certificado digital.

Si realizamos un símil con el mundo físico, estos sitios web eran accesados utilizando un "llavín" preparado para leer Códigos de Usuario y Palabras Claves. Solo habría que cambiar el "llavín" para que pueda leer la llave maestra: los certificados digitales. Pero por un tiempo razonable, hasta que todos los clientes puedan disponer de certificados digitales, estos sitios deben tener esquemas de Autenticación Duales o dicho de otra forma, "dos tipos de llavines", el tradicional y el que utiliza certificados digitales, en donde poco a poco vayamos desplazando a todos los usuarios de sistemas informáticos a utilizar estos nuevos instrumentos y dispositivos de seguridad.

La motivación para el cambio y la firma digital

La existencia de la firma digital nos abre una enorme gama de posibilidades a la hora de trasladar trámites, que han requerido hasta el momento de la presencia física del ciudadano, para llevarlos a ser realizados completamente como un proceso provisto por una infraestructura digital. Hoy en día, para abrir una cuenta corriente o de ahorro, para solicitar una tarjeta de crédito, un préstamo de dinero, la solicitud de un servicio público, entre muchos otros, requerimos de la presencia de la persona para, luego de identificarse, firmar la solicitud respectiva, para recibir el bien o servicio solicitado.

Con los certificados digitales y la posibilidad de firmar digitalmente cualquier operación, un ciudadano podrá potencialmente, en la medida que esos trámites sean ofrecidos en la red, realizar cualquier solicitud de un bien o servicio que actualmente debemos solicitar presencialmente, esto nos indica que, por ejemplo, un banco estaría en capacidad de ofrecernos llenar digitalmente las solicitudes para abrir cuentas en diferentes monedas, darnos un crédito, solicitar una

chequera, una tarjeta de crédito, realizar transacciones de fondos a clientes por cualquier monto, sin requerir de nuestra presencia física, todo con el debido respaldo legal.

Lo anterior nos indica, que los clientes que dispongan de certificados digitales, obtendrán de las entidades una muy amplia gama de nuevas funcionalidades, así como significativas mejoras a las operaciones ofrecidas actualmente a través de la Web, pero debemos ser claros, si el país no le ofrece a los ciudadanos una rica gama de servicios digitales que faciliten su vida, éste no tendrá los incentivos adecuados para hacerse de su respectivo certificado digital.

La firma digital certificada y los procesos de autorización

Al permitir acceso a un sitio web utilizando un certificado digital, emitido siguiendo las políticas nacionales, se tiene la confianza de estar tratando con la persona que dice ser, lo que fortalece en forma significativa el proceso de autenticación de usuarios y lo define como un esquema seguro y general para cualquier aplicación web nacional.

Al ingresar al sistema, éstos, automáticamente realizan la autorización, es decir, asignar al usuario derechos sobre determinadas funcionalidades, sobre las diferentes transacciones disponibles, criterios predefinidos en todo sistema de cómputo.

Ahora bien, entre la variedad de transacciones que el cliente tiene derecho a realizar, hay transacciones de muy diversos niveles de riesgo. Por ejemplo, al ingresar al sitio de nuestro banco, podría darse una valoración de riesgo diferente para la consulta del estado de cuenta que para las transferencias de fondos entre clientes, o bien, para la solicitud de la apertura de una nueva cuenta versus el pago de un servicio público convencional, por citar transacciones típicas.

La valoración completa de todas las transacciones disponibles desde una perspectiva de riesgos, puede requerir que un subconjunto de éstas deban ser firmadas digitalmente, para obtener el aval y compromiso definitivo del cliente al ser ejecutadas.

Según la Ley 8454, una transacción firmada digitalmente tiene validez jurídica ante el estado cuando ha sido generada utilizando

una Firma Digital Certificada, y como tal, puede ser utilizada para demostrar la autorización por parte del cliente de su voluntad al momento de su realización. Esto es, si una transacción fue realizada sin el consentimiento de un cliente, éste puede demandar por la presentación de la firma digital asociada a dicha transacción - si la institución que brinda el servicio no puede dar evidencia de que dicha transacción tiene asociada la firma digital del cliente, éste puede reclamar alguna retribución si dicha transacción lo afecta.

En sentido inverso, si la institución demuestra que la transacción tiene asociada la firma digital del cliente, éste tiene según la ley la carga de la prueba, ya que con la activación del principio de "no repudio" el cliente debería demostrar que efectivamente nunca ordenó dicho trámite.

Como comentario final a este apartado, se puede mencionar que la validez jurídica de las firmas digitales estipuladas en la Ley 8454, aplica única y exclusivamente para las firmas digitales producidas utilizando certificados digitales emitidos por una Autoridad Certificadora, debidamente acreditada ante el Ministerio de Ciencia y Tecnologías y cuya infraestructura tecnológica y de procesos haya pasado los exigentes controles de calidad del ECA (Ente Costarricense de Acreditación).

Visionando el mundo digital

Estamos en la construcción de una futura sociedad digital, formada por una gran cantidad de edificios web, los cuales ofrecen a los ciudadanos una amplia y muy variada disponibilidad de servicios electrónicos: los edificios de la banca en línea, brindando transacciones financieras para un cliente cada vez más exigente, los múltiples edificios digitales orientados a los trámites con las entidades públicas, los cuales nos permitirán tener una relación de mayor cercanía y confianza con instituciones de gran importancia para el bienestar del país, edificios diseñados para el apoyo de los servicios propios del comercio electrónico; todos estos edificios orientados a brindar al ciudadano facilidades con mayor calidad y oportunidad, redundando al final de cuentas en una mejor calidad de vida para todos al reducirle el consumo de tiempo y recursos en filas y traslados innecesarios.

En esta ciudad digital las ACs son equivalentes a los cerrajeros que tenemos en el mundo físico, encargados de entregar llaves maestras al ciudadano, para que éstos puedan ingresar a los diferentes edificios a realizar sus transacciones. La labor del cerrajero digital es compleja y muy delicada, requiere tener no solo una robusta infraestructura tecnológica, sino procesos que garanticen que el "no repudio" esta soportado en esquemas de muy alta calidad operativa y de procesos.

Solo imaginar lo peligroso que sería entregarle el certificado digital a la persona incorrecta y permitir que esta pueda suplantar la identidad de otro y realizar transacciones comprometiéndolo, es atroz.

Aunque potencialmente pueden existir varias AC, ya tenemos operativa y en funcionamiento la AC del SINPE, la cual como explicamos anteriormente emitirá certificados digitales a través de la Banca. Por otra parte, trabajamos en coordinación con los bancos para preparar un conjunto de sucursales, estratégicamente ubicadas a lo largo y ancho del país, para que sirvan de unidades de distribución de certificados digitales para los clientes bancarios -más de 2 millones- ya disponibles en algunas oficinas de las principales instituciones financieras del país, siendo un proceso que se irá consolidando a través del tiempo, y en donde la experiencia nos va a ir dando la pauta de cómo gestionar el negocio de la cerrajería digital.

Con respecto a la calidad y altura de cada edificio web, esto dependerá de las respectivas instituciones. Por más que dispongamos de llaves maestras robustas, si las funcionalidades transaccionales no existen, los certificados digitales y la firma digital no ayudarán en gran cosa. No se debe perder de vista que los certificados son únicamente la llave para entrar al edificio, el fin último es que existan edificios enormes, con muchos y variados servicios para el ciudadano. En otras palabras, no existe razón para la existencia de certificados digitales si no hay sitios web donde utilizarlos.

Los bancos por su parte están haciendo la tarea de preparar sus sitios web, para realizar autenticación de sus clientes utilizando certificados digitales y la firma de las transacciones de mayor criticidad para brindar seguridad jurídica a las mismas.

Esperamos que estas infraestructuras bancarias y del resto de las entidades financieras estén completas a partir del segundo semestre del año en curso.

Proyectando los siguientes pasos

En este ensayo he pretendido describir un problema, la existencia de múltiples esquemas de autenticación, prácticamente uno para cada sistema disponible, con las dificultades que esto tiene para el usuario, por otra parte una solución, el diseño y construcción del equivalente a una "Llave Maestra", una llave que nos permita ingresar a todos los sitios web nacionales, los cuales confíen en el respaldo y seguridad de este nuevo instrumento de acceso.

También, una estrategia para la emisión, distribución y entrega de dichas llaves, utilizando la infraestructura del Sistema Nacional de Pagos (SINPE) como emisor de los certificados digitales, y a las sucursales de las entidades financieras como centros de distribución de los mismos para con sus clientes.

Por otra parte, el número de sucursales preparadas para entregar certificados digitales estará directamente determinadas por la demanda de los mismos, siendo dicha demanda producto de los nuevos servicios ofrecidos en el mundo digital, en donde utilizar certificados digitales sea un requisito para su uso, en otras palabras, no tiene sentido el disponer de llaves si no existen puertas que abrir.

El reto que tienen entre manos las instituciones y empresas es significativo, pero los beneficios superan por mucho los costos asociados, la tarea es de todos, en la construcción de la sociedad digital todos somos actores, desempeñando diversos roles, ya sea como constructores o simples usuarios, en esta distribución de funciones, los cerrajeros digitales han venido haciendo su trabajo, aportando confianza a través de la puesta en marcha de esquemas eficientes y seguros, lo demás es tiempo y mucho trabajo.

¿Para que sirve la firma digital?

Luis Roberto Cordero Rojas

¿Qué tiene que ver la firma digital con ciberseguridad?

Pensar como se pueden cometer ciberdelitos utilizando este mecanismo; aquí estamos hablando de como aumentar la seguridad a través de la firma digital, si el componente como tal deja espacios a formas de criminalidad.

¿Qué es y para qué sirve la firma digital? Desde una perspectiva diferente, en que ayuda la firma digital para estar ciberseguro, ¿Cuál es el eslabón más débil?

Wikipedia define la ciberseguridad o seguridad de las computadoras como: "La rama de la tecnología conocida como seguridad informática aplicada a computadoras y redes. Los objetivos de esta rama incluye la protección de la información contra robo, corrupción o desastres naturales, pero permitiendo a su vez que la información y la propiedad de la misma sean accesibles y provechas para el usuario legitimado para usarla", ya no hay que ir a la enciclopedia británica, para consultar una definición. Los objetivos de esta incluyen la confidencialidad, la integridad y la disponibilidad de la información.

Debemos tomar en cuenta aspectos como las páginas web con túneles encriptados, la encripción de las bases de datos para acceder a la información que se considera confidencial y a la integridad de la información. Si la información esta encriptada pero no está disponible no sirve y si la información no esta encriptada pero tampoco está disponible de igual manera no sirve, entonces todo versa sobre el tema de la información, o sea uno podría decir que el tema de la ciberseguridad versa sobre la protección de la información en todos sus ámbitos si la acumulan y la manejan correctamente, incorrectamente o si la venden o la alteran.

Además hay que preocuparse por el tema de la información; por ejemplo una transacción en un banco, donde se traslade dinero de un punto A a un punto B es información, por lo que hay que ver como se protege. No todo tiene que ser confidencial, ni se necesita que todo sea secreto. Un documento que va a registro público para el traspaso de una propiedad necesita que sea integro o que este protegido contra cambios no autorizados, pero no necesariamente confidencial, de por sí va a entrar en una base de datos, en el cual se puede pedir una certificación, ya que al final esa información es pública.

Sobre el tema de la disponibilidad

A los informáticos no hay que explicarles el tema de la disponibilidad, conexiones redundantes, electricidad redundante y sistemas de desfragmentación redundantes, y resulta que todo lo anterior es posible proveerlo sin firma digital e inclusive con mecanismos más sencillos de implementar. Si esto es más fácil implementarlo sin firma digital entonces ¿por qué implementar firma digital?

La definición de la ley 8454: “entiéndase por firma digital cualquier conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento electrónico”.

La firma digital es el conjunto de la tarjeta, la llave maestra y lógicamente la certificación digital que permite verificar su integridad, así como identificar de forma unívoca al autor con el documento

electrónico, o sea es un tema de manejo específico de la información, procesando la información. La firma digital sirve para ligar una fórmula matemática con un juego de llaves o llave maestra a un documento. Una firma electrónica es aquella que dice acepta, le pone todo el contrato, páginas de páginas que nadie lee o muy pocas personas leen y al final digo dice acepto, eso es vinculante. En un cajero se digita el pin el cual es una firma electrónica, porque hay un contrato que dice que cuando usted digita su pin entonces acepta sacar dinero, transacciones y demás; esta es una forma de ligar una determinada información a una fórmula matemática, generada en una infraestructura especifica, como ahora le enseñaron, con protecciones especificas usando *hardware* criptográfico especializado.

La firma permite ligar una fórmula matemática a un documento, verificar la integridad de un documento e identificar al autor, hay algunas formulas para verificar la integridad. Algunas ventajas sobre el mundo físico es la firma, si se quiere corroborar esa firma se trae un perito, la otra parte también trae un perito que dice que esa es su firma y ahí pasa en los tribunales dando vueltas con los expertos diciendo si la firma es o no es, aquí hay mecanismos muy exactos para lograr esto.

Qué relación tiene la firma digital con la ciberseguridad, o tienen fines distintos. La ciberseguridad habla de la seguridad y la disponibilidad de la información, la firma digital habla de la vinculación jurídica de la información con su autor, porque lo que interesa es llevar un documento firmado digitalmente ante un juez; por ejemplo si deben dinero y si se firma un pagaré electrónicamente o digitalmente, resulta que el juez dice "no mire que si usted no me trae el documento con las dos firmas de puño y letra yo no le puedo aceptar eso y no lo puedo ejecutar", entonces usted pierde la plata. Se puede ver que la firma digital no necesariamente tiene el mismo fin que la ciberseguridad, es un asunto de establecer mecanismos que se acepten en cualquier institución del Estado y que sea realmente valido.

Tampoco son dependientes entre sí, ¿es factible ser ciberseguro sin firma digital? Sí se puede, si se maneja adecuadamente la información y se establece donde es confidencial, si es integra y se manejan todos los accesos a servidores web y ahí no les tengo que decir pared de fuego, detección de intrusos, control de bitácoras.

Entonces qué relación tiene la firma digital con la ciberseguridad, resulta que por la misma implementación de la tecnología hay elementos de la firma digital que fortalecen la ciberseguridad, no porque ese era su fin, si no por que como era implementada y no es establecida ella en sí misma. Por ejemplo en las bóvedas está bastante seguro y toda esta seguridad comienza a pernearse en el sistema, entonces la firma ayuda a estar más ciberseguro. Para poder firmar digitalmente se necesita el certificado digital, para obtener un certificado digital se necesita pasar por un proceso de registro riguroso y luego almacenar el certificado en un módulo seguro. Se debe pasar por un proceso de registro, apoyando la iniciativa de autenticación e identificación de usuarios a los sitios web, la firma digital en sí no sirve para acceder a los sitios web bancarios y eliminar el *pishing,* es el certificado digital no la firma.

¿Estamos más ciberseguros?

La firma es para vincular el autor con el documento, pero el certificado digital es una parte necesaria y fundamental del sistema, para generar un certificado digital se necesita un juego de llaves para ser más ciberseguro, ese mecanismo tiene que estar certificado por un ente extranjero, en este caso el FITS es un organismo conjunto de políticas informáticas en conjunto con Estados Unidos y Canadá que ellos también tienen sus propios mecanismos, pero que al pedir un mecanismo seguro, ya logró que ese mecanismo no solo este protegido de terceros, sino de ustedes mismos por que el mecanismo ya sea la tarjeta o el *token* no deja exportar ese mecanismo que asume que usted no es lo suficientemente cuidadoso para manejar ese secreto y luego el sistema correctamente construido garantiza un nivel mínimo de seguridad y confianza.

Todo el tema de las transacciones electrónicas, los certificados digitales y la ciberseguridad versa sobre dar más confianza en el sistema, cuando no confía en el sistema no usa ese sistema. Entonces siguiendo con esta pregunta de si ayuda a estar más ciberseguro o no. Seguimos extrayendo con firma digital, el tema de llaves también puede ser utilizado para encriptar la información, asegurando la confidencialidad, el mecanismo de certificado digital emitido también puede ser utilizado como mecanismo de identificación de

usuarios. También el tema de firma digital necesita que la información se mantenga íntegra para poder garantizar la vinculación jurídica, el tema de *anti-tampering,* o sea, al tomar una transacción se modifica y se vuelve a introducir dentro del canal, se puede configurar al sistema para que acepte solo certificados digitales, resulta que el proceso para la emisión del certificado recolecta una cantidad importante de la persona o bien del presunto ciberdelicuente, por que cuando se va emitir un certificado digital le toman la foto, le toman la huella y lo ponen a firmar.

El eslabón más débil

Al final no olvidemos el eslabón más débil sigue siendo el usuario final, porque también la firma digital podría ayudar a estar más ciberseguro. El sistema de firma digital se quiebra en dos puntos: la seguridad de la operación de las autoridades de certificación y los procesos de registro para la emisión de certificados. Pero desde una perspectiva de usuario, el mal uso del certificado (robo o descuido) y que la seguridad dependa en su totalidad del certificado, sin procesos adicionales de verificación.

La firma digital valida el proceso de registro, dan una tarjetita que se instala en el computador, se instalan *drivers* y se puede firmar digitalmente un documento con ese mecanismo, así se puede acceder a sitos financieros sin ningún problema, ya no hay que pasar por los múltiples mecanismos de los diferentes bancos. El MICIT tiene todo auditado, ahí no hay ningún problema. Existen tres posibles escenarios de ciberdelitos con la firma digital; fraude utilizando firma digital válida por mal uso o descuido, robo o intimidación y robo de identidad y *e-banking*.

Finalmente, la ciberseguridad y la firma digital introducen un elemento de inseguridad, se traslada la responsabilidad al usuario final de mantener seguro el sistema, es una necesidad o un riesgo inherente al sistema, están dando seguridad en muchos otros aspectos, pero no se deben descuidar los aspectos que ahora versan en el tema de las redes sociales, entonces al final quién es el que tiene la responsabilidad del riesgo, del manejo de información, el usuario final porque tiene que saber cuál es la información que puede dar; así como el manejo del dispositivo con el que se va a firmar.

Sistema Nacional de Certificación Digital

Oscar Julio Solís Solís

¿Por qué usar un sistema digital de confianza?

Todos sabemos que Internet presenta una serie de ventajas, pero a su vez conlleva muchos riesgos. Los riesgos los podemos ver materializados por ejemplo en el sistema de identificación y de autenticación que usamos para ingresar en los sitos de Internet, el cual consiste en un sistema de usuario y contraseña (*login y password*), lo que presenta amenazas tales como: suplantación de identidad, robo de información y fraude.

La solución que se busca a este problema es implementar mecanismos robustos de autentificación y firma para los usuarios. Ello se logra con la emisión de certificados digitales y las firmas digitales, ya que esta herramienta protege la identidad y vuelve las comunicaciones seguras. Es una autenticación confiable, con la cual Internet se vuelve más segura, en relación con las amenazas que se viven a diario al navegar por Internet. El *login y el password* se deben "pensionar", por razones de seguridad, es necesario dar un paso más al frente e iniciar con otro sistema. Necesitamos nuevos sistemas de identificación mucho más confiables y eficaces.

¿Por qué esta solución es mucho más segura?

En este sistema, la seguridad está basada en secretos (contraseña, pins, llaves). Es como las llaves que utilizamos para entrar a nuestra casa, con las combinaciones diferentes que esto implica, es un secreto, es una seguridad; pero los secretos se exponen, la información sensible viaja como lo vimos con el *login y el password*. Los secretos son muchas veces poco complejos, por lo que pueden adivinarse utilizando ataques de fuerza bruta (probando todas las posibles combinaciones), o usando diccionarios (palabras claves que bien definidas por defecto en los equipos o sistemas).

El último factor, tal vez el más importante y más delicado, es el factor de ingeniería social, o sea el factor humano, (que es el mal uso de por parte de los usuarios de sus secretos). Con el fin de prevenir estos problemas de seguridad es que se implementa el uso del certificado digital, resguardando el secreto en un dispositivo que tiene un microprocesador criptográfico que cumple con un estándar de seguridad que se denomina FIT140 nivel 2. ¿Qué quiere decir esto?. Que este dispositivo ante un acceso no autorizado o cuando haya intento de robo de la información contenida en él, prefiere eliminarla, es decir, si una persona intenta abrir físicamente el dispositivo para obtener el secreto contenido en él, a partir de cierto nivel de seguridad el dispositivo borra la información para no comprometer la integridad del secreto. Además el secreto posee una gran complejidad, lo que implica que a pesar de utilizar un ataque de fuerza bruta o intentando todas las posibilidades, no se puede descifrar la relación que existe entre los algoritmos matemáticos, entre la llave pública y la llave privada; además este sistema implica el uso de dos factores de identificación: algo que yo tengo que es el dispositivo y algo que yo se que es el pin de activación que yo mismo defino y que nadie más conoce.

En este momento el Banco Popular es el único ente que tiene un sistema en el que se utiliza el certificado digital de la Jerarquía Nacional. Hay otras instituciones que han venido trabajando en este proyecto y que han modificado sus aplicaciones, como por ejemplo el Ministerio de Hacienda con “Tributación Digital”, Compra Red y TICA, que

han hecho una excelente labor, al modificar y crear la infraestructura necesaria para crear aplicaciones que utilicen certificados digitales, porque al final esto es un medio, no un fin, el fin son las aplicaciones.

El factor de identificación es a través de una tarjeta, la cual si yo pierdo o entrego a otra persona, no la van a poder usar, ya que faltaría el pin o la clave de activación de la misma. Las obligaciones por lo tanto, no solo se tienen a nivel de las Autoridades Certificadoras, sino también implica la responsabilidad que tenemos cada uno de nosotros en nuestro papel de usuarios del Sistema Nacional de Certificación Digital (SNCD). Tenemos que proteger lo que nos identifica, lo que nos compromete, asumimos la misma responsabilidad que si estuviéramos firmando hojas en blanco, por lo cual debemos resguardar nuestro certificado digital, así como el pin de activación, de manera que si se pierde el certificado digital, debemos recovarlo ya sea a través de la página en internet o por medio del servicio de soporte que posee la autoridad certificadora para este fin.

El certificado digital

El certificado digital es un documento electrónico que relaciona la identidad de una persona con una llave pública. A nivel de desarrollo de aplicaciones para poder utilizar esta herramienta, lo más importante es que lo único que contiene respecto al usuario, es su nombre completo y su número de cedula de identidad. Con lo anterior, podemos indicar que los componentes principales del certificado digital son: el titular, una llave pública, un emisor, un identificador único, el período de validez y la firma digital del emisor, o sea, solamente contendrá información inherente a la persona.

En el dispositivo criptográfico la llave privada y el certificado digital pueden ser almacenados en tarjetas inteligentes y seguras. También se utilizan *"TOKEN USB"* para proteger la llave privada y el certificado de un titular. Por lo tanto el dispositivo criptográfico tiene mecanismos de autenticación. Las llaves privadas contenidas en el dispositivo, nunca son expuestas y tiene protección tanto física como lógica.

Como mecanismo criptográfico, a mediano plazo estamos apuntando a la cedula de identidad, a fin de que se de una confluencia entre

nuestro documento de identidad y la firma digital, tal y como sucede en Europa. Como conclusión a los párrafos anteriores, estos mecanismos son lo suficientemente robustos para proteger el secreto, lo que implica un factor que es esencial: es el no repudio a un documento firmado digitalmente.

La Autoridad Certificadora

La Autoridad Certificadora es un tercero de confianza que emite certificados digitales. La validez de un certificado digital dependerá de la confianza que se tenga en el emisor del mismo. Pueden existir muchas formas de crear y poner en funcionamiento una Autoridad Certificadora, pero la confianza que se de en ellas, dependerá de la forma en que la misma fue creada; puede tener una forma muy robusta y segura de crearla o incluso se puede montar una autoridad certificadora en una laptop y emitir certificados con los riesgos que esto implicaría, pero para que tengan la validez jurídica y para que sea una firma digital certificada y por lo tanto goce de la presunción de autoría que establece la Ley 8454, necesita cumplir con una serie de requisitos que se desprenden del documento de Políticas para la jerarquía nacional de certificadores registrados, así como las normas internacionales ISO/IEC 17021 y 21188.

La Norma Internacional ISO/IEC 21188 es una "Competencia Técnica" con controles ambientales como: capacidad de custodia, alta disponibilidad, personal de seguridad, monitoreo y recuperación de seguridad en casos de desastres. Además con controles de Administración como: gestión de dispositivos criptográficos, personal con roles de confianza mancomunados, implementación de servicios de validación y sistemas de gestión de la seguridad de la información.

La capacidad de custodia que debe tener una Autoridad Certificadora es muy grande. De igual manera debe contar con personal de seguridad apoyado por sistemas de monitoreo, así como una serie de controles (controles de administración, de los dispositivos criptográficos, que son para proteger la llave privada, que es de mayor seguridad que y volumen que el dispositivo criptográfico que se entrega a una persona, un *token* más robusto, más fuerte, que se denomina HSM

que es un Módulo de Seguridad *Hardware*). Los roles de confianza se desarrollan por mancomunación, para poder obtener el ingreso a la Autoridad Certificadora, ya que no puede ingresar una sola persona. Por ejemplo, para poder ingresar a la Autoridad Certificadora Raíz, que pertenece al Ministerio de Ciencia y Tecnología, se ocupa la participación de al menos un funcionario del Ministerio y dos funcionarios del Banco Central de Costa Rica; dos funcionarios del Banco Central no pueden abrir las bóvedas donde se hospeda la CA Raíz, ya que se ocupa la participación de algún funcionario del MICIT.

La norma 17021 es una "Competencia Administrativa" que implica un sistema de gestión de calidad, que exige que el personal que opera una Autoridad Certificadora tenga competencia, el conocimiento y la capacidad para hacerlo.

Modelo nacional

La Asamblea Legislativa entregó al MICIT la responsabilidad de emitir el reglamento a la ley 8454. En su oportunidad, el MICIT contó con la participación tanto del sector público como del privado (Poder Judicial, Cámara Costarricense de Tecnologías de Información y Comunicación (CAMTIC), el Registro Nacional, el Banco Central, el Consejo Nacional de Rectores (CONARE) y la Procuraduría General de la República, entre otras); instituciones que nos han apoyado para considerar al SNCD como un proyecto país.

Todo esto a nivel tecnológico tiene repercusiones jurídicas, porque la ley nos dice que los documentos y comunicaciones con firma digital certificada, tienen el mismo valor y eficacia probatoria que un documento firmado en manuscrito. El artículo 10 de la ley 8454, nos dice que todo documento firmado y asociado a una firma digital certificada, (que es la misma que se emite bajo una jerarquía y cumpliendo todos los requerimientos anteriormente indicados), se presumirá salvo prueba en contrario, de la autoría y responsabilidad del titular del correspondiente certificado digital. O sea si yo firmo algo utilizando mi certificado digital, se presume que es de mi autoría, porque el certificado digital esta a mi nombre y yo soy el titular del mismo, este nos da una identificación unívoca, una validez jurídica, eficacia probatoria, presunción de autoría y el no repudio.

Responsabilidades para el MICIT

Al Ministerio de Ciencia y Tecnología le corresponde una serie de responsabilidades que le fueron asiganadas por ley: la conformación de la Dirección de Certificadores de Firma Digital, la reglamentación a la ley 8454, la creación y publicación de políticas, la puesta en marcha de la raíz nacional, la coordinación con el Ente Costarricense de Acreditación y otras más que hemos venido desarrollando.

Entre los retos que tenemos que enfrentar podemos nombrar el romper con la brecha digital, creando una cultura digital tanto en el sector público como en el privado, motivar a todas las instituciones que modifiquen y creen aplicaciones para utilizar el certificado y la firma digital como herramienta. De igual manera incentivamos a Gobierno Digital, que en varias oportunidades ha mencionado que tiene varias aplicaciones listas para utilizar la firma digital, que las ponga en funcionamiento a la mayor brevedad.

Tenemos que dar un paso adelante, el masificar el uso de la firma digital como herramienta no puede ser de la noche a la mañana, ya que no es cualquier implantación de tecnología; es un desarrollo que se debe dar de manera paulatina, por lo que necesitamos toda la ayuda posible para poderla implementar a nivel nacional.

Capítulo 4
Tipo y naturaleza de los ciberdelitos

Ciberdelitos: tipos y soluciones

Christian Hess Araya

Este es un tema de enorme actualidad. Todos los días estamos viendo en las noticias información con relación al tema de los delitos informáticos y hace poco éstas revelaron un hecho importante: que la empresa Microsoft fue víctima de un ataque de phishing resultado del cual se denunció que por lo menos 10000 contraseñas de las cuentas de Hotmail y en general del sistema Windows Live fueron sustraídas y dadas a conocer públicamente en blogs de Internet.

Este fue el resultado de un ataque de phishing en Internet, que es una forma de ciberdelito. Algunos expertos en la materia temían que éste fuese solo la punta del iceberg de un fenómeno más grande, que podría afectar no solo a Microsoft sino también a otros proveedores de Web Mail como Gmail, Yahoo, etc.

Este es un ejemplo clarísimo del interés actual que tiene el tema de los ciberdelitos.

Tipología de los delitos informáticos

Delito informático

- Sentido objetivo: el delito recae sobre objetos del mundo de la informática.
- Sentido funcional: la informática es empleada como herramienta o instrumento para el crimen.

"Delito informático" es una expresión que tiene dos sentidos, dos acepciones, dos ángulos posibles desde los cuáles se puede enfocar el tema de los ciberdelitos.

Desde una perspectiva objetiva, vamos a considerar como delito informático a cualquier fenómeno ilícito, cualquier conducta atípica, antijurídica, prevista en la legislación penal, donde el objetivo del delito es un bien o servicio propio del mundo de la informática. Por ejemplo, insertar un virus en una computadora para alterar el sistema, es un delito informático enfocado desde esta perspectiva.

La segunda perspectiva es la funcional, donde el sistema de cómputo ya no es el blanco de la conducta delictiva, sino apenas una herramienta para cometer ilícitos contra terceras personas. Así como un delincuente puede servirse de una "pata de chancho" para abrir una ventana e introducirse a una casa, un delincuente también puede servirse de un bien o servicio informático para un fin ulterior: extraer dinero de una cuenta bancaria, alterar información, etc.

Esta segunda acepción tiene un significado más amplio, más genérico que la primera, aunque debemos evitar en todo caso llevarla al extremo. Hay alguna jurisprudencia nacional, por ejemplo, existe una sentencia de la Sala Tercera del 2006 que nos previene sobre utilizar demasiado ampliamente esta acepción del delito informático, para entender de alguna manera que no todo lo que tiene que ver con una computadora es un delito informático, eso sería falso.

Por ejemplo, si un delincuente quiebra un cajero automático para robarse el dinero, eso no sería un delito informático, por más que el cajero sea una especie de computadora o equipo tecnológico; esto sería emplear excesivamente el sentido funcional del concepto.

Dificultad de persecución

- Factor velocidad
- Factor geográfico (distancia)
- Facilidad de encubrimiento
- Indiferencia de la opinión pública
- Temor a denunciar los delitos
- Perfil no tradicional del delincuente

Los delitos informáticos, a diferencia de los delitos tradicionales, se caracterizan, entre otras cosas, por su dificultad de persecución. Lo difícil es identificar la comisión del delito, al autor o autores del delito, perseguirlos, o sea someterlos a la acción de la justicia y eventualmente condenarlos. Esto se debe a una multiplicidad de factores que conspiran en el caso de los delitos informáticos para este propósito, a diferencia de los delitos tradicionales.

Los delitos informáticos son cometidos con gran celeridad, en cuestión de microsegundos es posible cometer masivamente delitos informáticos a diferencia de lo que ocurre con la mayoría de los delitos en el mundo físico, donde hay cierta planificación hay cierto iter delictivo que toma minutos, horas, días etc. Un delito informático se ejecuta muy rápido por lo tanto es difícil impedirlo, es difícil detectarlo, por este factor.

Un segundo elemento es el factor geográfico, la distancia. A diferencia de los delitos del mundo tradicional donde, por ejemplo, para cometer un homicidio, uno tiene que acercarse físicamente a la víctima, en el mundo de la informática es posible cometer delitos desde el otro lado del mundo, a través de las redes telemáticas -y en particular de Internet- es posible poner el factor distancia entre el autor y la víctima o víctimas del delito.

Esto complica todavía más la cosa, porque le da un carácter transnacional al fenómeno de la delincuencia informática y eso complica siempre las cosas en el plano jurídico, porque involucra múltiples jurisdicciones, legislaciones, organismos policiales de investigación, etc.

La facilidad de encubrimiento es otro factor que complica mucho las cosas en la medida que cualquier persona que tenga los conocimientos y las habilidades necesarias le permite además de cometer el delito, encubrirlo también, o sea borrar las huellas del delito.

Por ejemplo si una persona tiene el carácter de administrador de un sistema de redes, tiene acceso a las bitácoras de seguridad, y a registros necesarios, a todo el sistema de defensa por decirlo así de un sistema informático, por lo tanto tiene acceso a la posibilidad de borrar sus huellas del delito, a diferencia de lo que ocurre en el mundo tradicional donde -para volver al ejemplo que di antes de un homicidio- luego de la comisión del ilícito hay un cadáver, hay sangre, hay señas de violencia, hay un arma homicida, etc. En el caso del delito informático, ¡la computadora no queda sangrando, ni se queja, etc.! Esto complica su persecución.

Luego tenemos un factor importante que es la indiferencia de la opinión pública. La presión de la opinión pública no es la misma, obviamente -y en alguna medida es correcto que así lo sea- en lo relativo a la importancia, la trascendencia que se da al fenómeno de los delitos informáticos, en contraste con la que se da a los delitos tradicionales. Cuando se comete un delito tradicional -sobre todo si es muy sonado; para poner un ejemplo, este caso de la violación de una muchacha en una fiesta- eso ha estado mucho tiempo en los medios de una forma constante; la opinión pública ha estado muy pendiente del tema; se exige que haya justicia, que se descubra lo que pasó realmente, que se sancione a los culpables, si es que son culpables, etc. Pero frente a los delitos informáticos, a los fraudes bancarios, a las intromisiones no autorizadas en bases de datos, la indignación pública no es tan fuerte en cuánto a exigir soluciones y por lo tanto los organismos policiales, los tribunales de justicia, etc., no están con tanta presión del público para obtener soluciones en este caso.

Por otro lado, en muchos de estos casos hay temor a denunciar estos delitos. Las empresas que son víctimas de estos delitos informáticos suelen ser renuentes a reconocer que han sido víctimas de un fenómeno de éstos, porque eso es altamente vergonzoso desde el punto de vista de ciertas empresas, sobre todo si tienen componentes tecnológicos importantes, como puede ser el caso de una empresa

comercial grande, o de un banco. Que se sepa que han sido víctimas de un delito informático es altamente embarazoso; puede exponer a su junta directiva, a investigaciones, etc. Entonces hay a veces una inclinación en algunas empresas a que, aunque hayan sido víctimas de un delito, sencillamente "lo dejamos tapadito, pasamos a perdidas lo que se haya ido, lo mejor es que nadie se entere, a que suframos la exposición pública correspondiente".

Y finalmente entra también en juego que el delincuente informático no suele tener el perfil tradicional del delincuente común. Es decir, el delincuente común -esa figura que, como dicen popularmente, uno no quiere encontrarse en un callejón oscuro a media noche- ese perfil tradicional del delincuente común no es el mismo del delincuente informático. Al contrario, el delincuente informático suele ser una persona de gran conocimiento, educación, con formación universitaria, con un nivel de vida bueno, con pleno acceso a posibilidades de diversión, no es necesariamente alguien que esté ahí de vago todo el día.

Por eso sucede que en los delitos informáticos uno nunca ve un retrato hablado del perpetrador. No hay alguien que haya hecho un retrato de un delincuente informático, primero, porque no lo ve; segundo, porque si se hace un retrato hablado de un delincuente informático posiblemente coincida con muchos de nosotros de los que estamos acá, así es que no ayuda mucho este elemento.

Clasificación

Así como les decía antes que los delitos informáticos podemos verlos en una doble acepción, como conducta objetiva o como conducta funcional, podemos aprovecharnos de eso para hacer una clasificación básica de los delitos informáticos.

Entonces, según estemos hablando del plano objetivo del delito informático, podríamos hablar de delitos que se han cometido contra el hardware, es decir de delitos cuyo objetivo es dañar equipos desde el punto de vista físico; así como la gran cantidad de delitos que existen contra sistemas de información, cuyo objetivo es interrumpir o dañar el procesamiento que está en cualquier sistema de datos, como puede ser el sabotaje informático, introducir un virus deliberadamente en un sistema.

En el segundo caso estamos en el plano funcional, donde la informática es sólo la herramienta para dañar a otro tipo de bienes jurídicos, también podemos hablar de los casos en los que la víctima es uno o más sujetos determinados. Como puede ser en algunos casos delitos de propiedad intelectual, donde hay un titular de los derechos de la propiedad intelectual que es la víctima del delito o bien ciertos delitos que son cometidos de forma genérica contra los intereses colectivos, donde el propósito no es dañar el interés o intereses de una persona en particular, sino como quién dice "tirar con escopeta" y provocar el mayor daño posible a sujetos indiferenciados, como pueden ser los casos de ciberterrorismo, divulgación por medios informáticos de pornografía infantil, etc. Es una rápida tipología de los delitos que existen dentro de esta materia.

Soluciones y tendencias legislativas

En cuanto a las soluciones normativas que se dan al fenómeno de la delincuencia informática, uno puede visualizar en el mundo diferentes clases de tendencias. Es decir, según la forma en que un país decida tratar el fenómeno de la delincuencia informática, vemos por lo menos ciertas tendencias básicas a nivel mundial.

Unos países optan por considerar a los delitos informáticos como conductas novedosas; es decir, como tipos penales diferentes a todos los que tenemos anteriormente, esto es, a los llamados tipos tradicionales.

Otra posibilidad que se vislumbra en los países es la de considerar a los delitos informáticos sencillamente como una manera nueva de cometer delitos tradicionales. Entonces, por ejemplo, los fraudes informáticos pueden ser considerados una manera nueva de cometer el tradicional delito de estafa, por lo que optan por cambiar o modular la definición pertinente para acomodarla a su comisión por medios tecnológicos.

Cuando estamos en el primer escenario, existen a su vez dos posibles alternativas. La primera es considerar al delito informático como una figura penal única y entonces en ese caso lo que se hace es introducir en la legislación un artículo penal nuevo con esa descripción. En el segundo enfoque, donde estamos hablando de conductas novedosas que a su vez se consideran tipos penales múltiples, lo que se hace en este caso es introducir en el Código Penal un capítulo

nuevo sobre delitos informáticos, con los múltiples enunciados correspondientes, o bien se promulgan leyes especiales que regulen las diferentes modalidades de comisión del delito.

Sí estamos en el último escenario de las conductas tradicionales, entonces en ese caso obviamente lo que se tiende a hacer es a reformar los artículos ya existentes o bien lo que se hace es agregarles incisos para regular las modalidades de comisión de esos delitos por vías tecnológicas.

Algunos ejemplos, en cuanto a países que hayan promulgado leyes especiales para regular el fenómeno de la delincuencia informática, incluimos a Venezuela, Chile, Estados Unidos, Alemania, entre otros.

Países en los que se ha reformado el Código Penal para añadir nuevos artículos o incisos: por ejemplo tenemos a Paraguay y tenemos a España con el Código Penal en vigencia (sí mal no recuerdo) desde 1995, en el que hay toda una regulación sobre los delitos informáticos.

Entre los países que han optado por introducir un capítulo nuevo especial para tratar los delitos informáticos tenemos a Bolivia y Francia.

Y en los países que han optado por una combinación de enfoques, tenemos por ejemplo a Argentina, Brasil y Costa Rica en lo que interesa. Es decir nosotros hemos optado, como que no hemos tomado una posición clara en cuánto a estas tendencias sobre como regular los delitos informáticos y hemos optado por un poquito de todo como lo voy a enunciar rápidamente ahora.

Situación Nacional

- Código Tributario (1995 y 1999) Artículos 93 a 97
- Ley General de Aduanas (1995) Artículos 221 y 222
- Legislación sobre derechos de autor
- Ley de Procedimientos de Observancia de los Derechos de Propiedad Intelectual (2000)

En Costa Rica, a partir de 1995 se comenzó a introducir la regulación de los delitos informáticos, primero a través de los artículos 93 - 97 del Código de Normas y Procedimientos Tributarios. Ese mismo año, en la nueva Ley General de Aduanas se añadió también

una serie de tipos referentes a la delincuencia informática. En el año 2000 se introduce una legislación importante, sobre todo en la protección de derechos de autor y en la Ley de observancia de los derechos de propiedad intelectual.

Ley de Administración Financiera de la República (2001) Artículo 111

Código Penal (2001)

- Artículos 196 bis "Violación de comunicaciones electrónicas"
- 217 bis - "Fraude informático"
- 229 bis - "Alteración de datos y sabotaje informático"

En el año 2001 tuvimos la promulgación de la Ley de Administración Financiera y de Presupuestos Públicos, donde hay un artículo relacionado con el tema de delincuencia informática. Luego se da la introducción de tres normas especiales al Código Penal sobre violación de comunicaciones electrónicas, fraude informático y alteración y sabotaje informático.

Con este último hubo un problema que se produjo no mucho después, en el año 2002, el legislador nuestro introdujo una reforma al Código Penal, en la cual promulgó un nuevo tipo penal con el mismo número este del sabotaje informático, el 229 bis, dando lugar a una discusión de si había derogado tácitamente o no el tipo penal del sabotaje informático. Esa discusión se ha venido dando desde varios años. En particular soy de una posición de que sí se dio una derogación tácita -equivocada, pero derogación al fin y al cabo- del tipo penal de sabotaje informático.

Propuestas de Lege Ferenda

- Ley de reformas al Código Penal
- Expediente 11.871
- Proyecto de "Ley de Delito Informático"
- Expediente 15.397
- Proyecto de "Adición de nuevos artículos al Código Penal para regular el delito informático"
- Expediente 16.546

Aparte de esas reformas legales ha habido una serie de propuestas que han sido presentadas en la Asamblea Legislativa.

Hay un proyecto de reformas al Código Penal que estaba ahí en la Asamblea Legislativa, presentado por el Poder Ejecutivo, que contiene una serie de regulaciones en esta materia. Desgraciadamente este proyecto de ley fue archivado por un tema de inactividad legislativa, que es cuando un proyecto pasa demasiado tiempo en trámite legislativo sin que se avance, entonces se archiva automáticamente y desgraciadamente pasó esto con este proyecto de ley.

Luego hubo un proyecto que en el 2003 propuso la entonces diputada María Elena Núñez Chávez que quiso regular el tema de los delitos informáticos. Éste es un proyecto que particularmente desconozco donde se encuentra en la Asamblea Legislativa, sí está durmiendo el sueño de los justos o no, pero realmente sería una pena, porque es un proyecto de ley bastante bueno, que tiene una redacción muy completa sobre esta temática.

En el 2007, la todavía diputada Lorena Vásquez introdujo en la Asamblea Legislativa un proyecto de ley de adición de artículos al Código Penal para regular el tema del delito informático, pensando básicamente en el tema de los fraudes de las tarjetas de crédito y algunos otros de manipulaciones de información bancaria y financiera.

Fenómeno transnacional

"Convención Europea sobre Ciberdelincuencia", noviembre 2001

- Está abierta a otros Estados no europeos
- Entró en vigencia el 1 de julio del 2004
- Costa Rica ha expresado interés en adherirse

Para ir terminando, les recuerdo lo que les decía al inicio, de que la delincuencia informática es un fenómeno transnacional y por lo tanto no es de sorprender que también haya habido esfuerzos por regular el tema a nivel internacional.

El esfuerzo más importante de todos estos es, a mi juicio, el "Convenio de la Unión Europea sobre la ciberdelincuencia", que es el primer instrumento multinacional diseñado para atacar el problema de

la ciberdelincuencia. Lo interesante es que a pesar de ser un convenio europeo está abierto a la adhesión de Estados no europeos. Últimamente, países como Estado Unidos, Japón, Cañada y Sudáfrica, se han adherido al convenio luego de que entró en vigencia el 1 de julio de 2004.

He escuchado en algún momento del interés de algunas autoridades nacionales de que Costa Rica se adhiera al convenio europeo sobre ciberdelincuencia. Por lo menos supe de un cruce de comunicaciones en la Cancillería donde se planteaba el tema de la adhesión de Costa Rica al convenio. Ignoro también -y si alguien tuviera ese dato sería interesante saberlo- si en el marco de las negociaciones del tratado de libre comercio con la Unión Europea, se está discutiendo o no el tema de la adhesión al convenio Europeo, pero sería interesante sí así lo fuera.

Comentarios finales

- Actualizar el marco normativo es una tarea urgente
- Unificar criterios jurisprudenciales
- Pero no es solo un tema jurídico, sino también de educación

Y ya termino con unos comentarios finales, en el sentido de que ya he tenido la oportunidad -y lo hago de nuevo cada vez que tengo chance de participar en una actividad como estas- de enfatizar de que en Costa Rica hemos tenido un enfoque, como les decía ahora, completamente confuso e inconsistente con relación al tratamiento de los delitos informáticos y hemos terminado en nuestra legislación con lo que yo llamo una verdadera “ensalada normativa”. Tenemos leyes especiales, algunos tipos generales en el Código Penal, proyectos de ley que pretenden regular de manera especial algunos tipos, etc.

Lo que nos ha faltado es una visión de conjunto para enfocar el tema de los delitos informáticos. Esto explica el hecho de que la jurisprudencia sobre delincuencia informática no siempre ha sido uniforme en cuanto al tratamiento de estos temas. Quizás haya un poco de desconocimiento de tratamientos judiciales en cuanto al tema, lo que hace que existan algunas soluciones contradictorias.

Entre los más sonados hoy en día, están los de los fraudes bancarios. Se ha tendido a utilizar un concepto de fraude informático, que

estrictamente y en puridad de términos coincide más bien con un tipo diferente, que es el hurto informático, que es una figura no prevista en nuestra legislación en el Código Penal; entonces tiende a tratar de forzarse conductas que corresponden más al hurto informático, dentro del fraude informático, de una forma indebida o incorrecta.

Luego está el hecho de que nuestro ordenamiento jurídico no prevé algunas figuras informáticas delictivas de gran actualidad. No hay una clara identificación de tipos como el phishing o el pharming, etc. Hay una serie de conductas de gran actualidad que no están claramente previstas en la legislación, que podrían ser clasificadas como modalidades de la estafa que sí está tipificada en el Código Penal.

En definitiva debemos de recordar que el tema del tratamiento de la delincuencia informática no es solo un tema jurídico; no es un tema que se resuelva solamente promulgando más leyes, sino que también es un problema que requiere de educación, particularmente educación del gran público en general sobre el uso seguro de la tecnología.

Estamos empezando a dar pasos importantes hacia delante. Desde mi perspectiva, uno de los pasos más importantes que se ha dado es la inauguración del Sistema Nacional de Certificación Digital, que es un elemento importante en el combate de fraudes bancarios y algunos casos de suplantación de identidad. Pero hace falta que el público, que el gran público sepa más del tema y sea educado. Esto incluye la educación a nivel escolar y colegial: hay que enseñarle a los jóvenes y a los niños como utilizar la tecnología en una forma segura, bajo el principio más que evidente de que los delitos informáticos -al igual que cualquier otro delito- es mejor prevenirlos, que después tener que perseguirlos y castigarlos.

Derecho penal económico

Carlos Chinchilla Sandí

El ciberdelito tiene que ver en realidad con el derecho penal económico, que aquí en Costa Rica es desconocido, porque lamentablemente es moderno para nosotros pero en Europa ya tiene 20 años de estarse desarrollando científicamente.

Delitos económicos

Todo esto tiene que ver con los delitos económicos los cuales tienen una característica que los identifica que son parte de los delitos informáticos y entonces se habla de delitos de TI, la gente se asusta porque no se necesita de un resultado para sancionar a alguien penalmente, ¿por qué? Porque aquí lo que podría ser la tentativa de un delito de resultado que es tomar una pistola dispararle al enemigo y el resultado es una persona muerta- pero del otro delito no hay un resultado que se pueda ver materialmente pero si se puede ver un peligro.

Sociedad del riesgo

- Progreso y desarrollo en la sociedad crea una serie de riesgos
- Riesgos asumidos socialmente
- La industrialización, el tráfico automotor, actualmente Internet
- Incremento del riesgo
- Generación de conductas delictivas

Todo esto tiene que ver con la sociedad del riesgo, con la Sociedad de la Información y el Conocimiento porque nuestras sociedades son altamente riesgosas y parece mentira entre más desarrollada sea una sociedad, más peligros genera, entre más rudimentaria y atrasada sea menos peligro genera. Principalmente la cuestión tecnológica nos ha generado una serie de beneficios que se vuelven peligrosos; el uso de Internet es un instrumento muy bueno para tener una información actualizada cosa que antes era bastante limitada, pero esta es una red que genera mucho peligro y provoca algunas conductas delictivas.

Delitos económicos, tiene que ver mucho también con delincuencia organizada y con los delitos informáticos, por lo que hay que tomar en cuenta que no siempre el que pensamos es el sujeto activo, no necesariamente es el informático manipulando un sistema directamente, pero sí hay detrás de él una red de delincuencia que tiene estos conocimientos para lograr esa conducta que se busca.

Delitos informáticos

Delitos informáticos, se habla por un lado de la informática y por el otro de las telecomunicaciones que nos da la telemática. Los delitos en términos generales son la acción delictiva que comete una persona, persona física, porque en Costa Rica aún no se ha evolucionado con lo que son delitos con personas jurídicas, en Europa es muy común hay muchas objeciones de carácter constitucional, pero esas objeciones son falacias, pero aquí nos negamos a aceptar todavía que las personas jurídicas son delincuentes y como delincuentes hay que tratarlos.

Delito informático: *La acción delictiva que realiza una persona con la utilización de un medio informático o, lesionando los derechos del titular de un elemento informático (se trate de las máquinas -hardware- o programas -software-).*

El delito informático tiene dos partes: una cuando se están violentando los derechos de un elemento informático ya sea el software o el hardware y siempre una acción de carácter delictiva. Y la otra cuando no solamente se habla el carácter delictivo sino de la intención con que realiza la acción -dolo- sino también del que por culpa o imprudencia por una acción de cuidado faltando a la acción de un deber comete el hecho delictivo y ahí hay sanción penal lógicamente.

¿Cuáles sujetos van a participar en la actividad criminal? Hay dos partes uno el sujeto activo y el sujeto pasivo.

Características del sujeto activo

- Poseen importantes conocimientos de informática
- Ocupan lugares estratégicos en su trabajo, donde se maneja información importante

El sujeto activo no necesariamente posee amplios conocimientos de informática, puede existir detrás de él hay una red o por lo menos personas que conocen de informática y le permiten utilizar algunos de estos elementos para realizar conductas delictivas.

Esto es muy importante estas personas ocupan un lugar estratégico en su lugar de trabajo sea una empresa privada, sea una institución pública, si ocupan importantes lugares pero no estoy hablando de jerarcas, estoy hablando de mandos medios cuidado y no un poquito más bajos. ¿Qué es lo que ocupa? Tener un lugar estratégico tener acceso al sistema, entrar en lugares donde está vedado para la mayoría introducirse.

- Puede tratarse de sujetos diferentes
- El joven que ingresa para vulnerar la seguridad *(hacker).*
- El empleado de institución financiera que desvía fondos de las cuentas de clientes.

Se dice como sujeto activo a los *hackers,* terminología que ha correspondido en algún momento a los delincuentes informáticos, se ha venido a acuñar la misma idea de *hackear*, de introducirse ilícitamente, son muchachos jóvenes que andan en edades de 13-14 años de 18 o 19 pero que ya se jubilan a los 20, porque resulta que ese *hacker* paso una línea divisoria entre el bien y el mal que es la línea que caminamos todos los días y nosotros decidimos irnos por el bien. Pero a veces la tentación de pasar al mal es tan cercana como no tener la colegiatura de la los niños, el alquiler de la casa, o tener necesidades imperiosas que provoca conductas delictivas.

Un *hacker* verdadero no es un universitario con muchos títulos y doctorados, no, es un genio ya de por sí. Diferente tipología del delincuente informático. Se dice que el nivel educacional en el ámbito informático no es indicativo. Otros consideran que son personas inteligentes, motivadas. Habíamos dicho que el sujeto activo tiene cierta caracterización, pero cabe destacar que aquí el nivel educacional no puede ser un indicativo de que la persona es un delincuente informático. Pero si tienen que ser personas inteligentes y motivadas a cometer un delito.

El sujeto pasivo: *Es la persona o entidad sobre la cual recae la conducta que realiza el sujeto activo.* La mayoría de delitos informáticos no son descubiertos porque no son denunciados por empresas o bancos, temen desprestigio y consecuente pérdida económica.

- Los sistemas penales persiguen con alguna eficacia, los delitos convencionales.
- Resultado difícil que se logra perseguir y evitar la impunidad, en el caso de los delitos no convencionales.
- Como delito no convencional tenemos a los “delitos de cuello blanco”. Llegamos al sujeto pasivo, que es lo que recibe la parte perjudicial o dañina del hecho delictivo.

Esta persona pasiva pueden ser entidades o personas físicas pero en general, cuando hablamos de entidades resulta ser que engrosan la cifra dorada de la criminalidad, porque son conductas delictivas que no son denunciadas.

¿Qué características tienen los delitos informáticos? La rapidez con que se cometen. Acercamiento en espacio, muchas veces o la gran mayoría de las veces hay un acercamiento del sujeto que comete el hecho con la víctima, pero muchas veces puede estar distante, hay facilidades de cometer el hecho y facilidad en borrar las pruebas.

Fraudes informáticos

Es importante hablar de fraude en delitos informáticos no es lo mismo que hablar de fraude legal, que quiere decir esto, que el fraude en delitos informáticos va más allá de lo que va en derecho penal. Existe confusión entre los conceptos de fraude informático y la estafa informática. No es lo mismo fraude informático que estafa informática. Los fraudes informáticos son el genio y las estafas informáticas son la especie. Entonces no todo fraude informático es una estafa informática pero que sí toda estafa informática es un fraude informático.

En realidad si ustedes ven la literatura informática muchas veces un fraude informático puede ser un hurto informático, un sabotaje informático o un daño informático. Por eso muchas veces limitar el nombre que se le da un delito para ubicar lo que es algo tan grande como el fraude no es correcto.

Tipos penales informáticos y legislación en Costa Rica

¿Dónde tenemos legislación en Costa Rica? La tenemos en varias partes:

- Código penal
- Ley de aduanas
- Código de normas y procedimientos tributarios (ley de justicia tributaria).
- Ley de derechos de autor y conexos
- Ley de la administración financiera de la república y presupuestos públicos.

Todas estas excepto la ley de derechos de autor tienen la misma normativa, es el mismo artículo cambiado en el Código Penal Artículo

196 bis. Violación de comunicaciones electrónicas: *"Será reprimida con pena de prisión de seis meses a dos años, la persona que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere, accese, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino, mensajes, datos e imágenes contenidas en soportes: electrónicos, informáticos, magnéticos y telemáticos. La pena será de uno a tres años de prisión, si las acciones descritas en el párrafo anterior, son realizadas por personas encargadas de los soportes: electrónicos, informáticos, magnéticos y telemáticos".*

En el artículo 196 bis se protege más que todo el ámbito de la privacidad, se recoge bien pero tal vez hay algunos elementos que van a dar al traste con ello porque dice que la pena será de uno a tres años de prisión, si las acciones descritas en el párrafo anterior, pero es que no hay párrafo anterior. Lo que hizo el legislador fue copiar un artículo que tenía varios párrafos y se olvido cambiar la frase, por lo que podríamos decir que el agravante no es aplicable en algunas formas, pero aún no lo hemos aplicado por lo que no tenemos interpretaciones al respecto.

Código Penal, artículo 229 bis. Alteración de datos y sabotaje informático: *"Se impondrá prisión de uno a cuatro años a la persona que por cualquier medio accese, borre, suprima, modifique o inutilice sin autorización los datos registrados en una computadora. Si como resultado de las conductas indicadas se entorpece o inutiliza el funcionamiento de un programa de cómputo, una base de datos o el sistema informático, la pena será de tres a seis años de prisión. Si el programa de cómputo, la base de datos o el sistema informático contienen datos de carácter público, se impondrá pena de prisión hasta de ocho años".*

En el artículo 229 bis sobre la alteración de datos y sabotaje informátic; en realidad el tiene un problema: vino un hermano gemelo de él, que también era el 229 bis que se llamó abandono dañino de animales y cayó sobre este, la naturaleza no tiene que ver nada, una cosa es un animal y otra cosa es quién comete alteración y sabotaje

de datos informáticos. Pero en realidad surge un problema la procuraduría trató de arreglarlo diciendo que era un solo artículo donde había una parte primera y una parte segunda donde la primera era de los delitos informáticos y la otra era de los animales, pero no servía porque no derogó la norma por lo cual debe interpretarse que la misma fue subderogada y no porque los contenidos son totalmente distintos y entonces esa técnica no se puede aplicar. La sala constitucional llegó a declarar inconstitucional el delito de abandono dañino de animales, no fue que esta norma fue derogada sino que este artículo nunca existió.

Dentro de la idea del sabotaje y alteración de datos informáticos la primer parte se refiere a la alteración y violación de una computadora; la segunda parte habla del sabotaje informático, pero surge un problema, tenemos una pena básica, una segunda que es agravada y una tercera que dice que cuando se trate de actos de carácter público la pena en prisión será hasta de 8 años, cuando dice hasta de… lo que quiere decir es que no podría ser menos que el agravante anterior penal, esto es lo que se interpreta, pero esto no debería dejarse como interpretación del juez debería darse de forma clara.

Código Penal, artículo 217 bis. Fraude informático: *"Se impondrá prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema".*

Habíamos dicho que no es lo mismo fraude informático, que estafa informática, esto es una estafa informática pero vean que interesante castiga de 1 a 10 años que es la misma pena que se le da a la estafa, pero esto no tiene sentido, tiene que ser una pena superior por el medio que se utiliza para cometer ese tipo de estafa, pero además de eso habla de influir en el procesamiento de los datos. Dónde dejaron el ingreso de los datos, pero ellos dicen que el ingreso de los mismos lo pueden entender como el procesamiento de los datos; no es posible aplicar eso, el juez no puede complementar las normas

penales, tiene que aplicarlas tal y como están, hay ahí un rango de interpretación pero el juez no puede crear tiene que aplicar.

El conflicto con el ingreso de los datos es que representan un 85% del problema de los fraudes que se dan en Internet, con lo que podría quedar fuera por decir que el procesamiento de los datos es lo mismo que el ingreso de los datos.

Propuestas de reforma Lege Ferenda, propuestas penales para Costa Rica:

1. Violación de datos Personales.
2. Abuso en el uso de los medios Informáticos.
3. Suplantación de identidad.
4. Hurto agravado.
5. Estafa informática.
6. Espionaje informático.
7. Uso de virus (software malicioso -Malware-).
8. Clonación de páginas electrónicas (páginas web).
9. Suplantación de sitios web para capturar datos personales (casos del phising y pharming).
10. Daño informático.
11. Sabotaje informático.

Violación de datos personales

Artículo 196 bis: *"Será sancionado… quien, con peligro o daño para la intimidad de las personas y sin su autorización, se apodere, abra, acceda, copie, transmita, publique, recopile, use, intercepte, retenga, suprima, oculte, desvíe, venda, compre, o de un tratamiento no autorizado a las comunicaciones, imágenes o datos de otra persona física o jurídica no públicos o notorios, a soportes informáticos, a programas de cómputo o a sus bases de datos".*

Bueno esto es parte de lo que se pretende modificar de alguna forma, entonces el artículo 196 que va a seguir siendo bis, un poco más completo sí se puede decir, aquí habla de una parte que me parece importante aquí, habla de lo no autorizado, pero tiene esta

parte que dice: **Violación de datos personales**:…*"En la misma pena incurrirá quien, contando con la autorización del afectado, recolecte los datos personales y los desvíe para un fin distinto para el que fueros recolectados…* La misma pena incurrirá quién contando con la autorización del afectado recolecte los datos y desvíe los datos del fin para el que fueron recolectados"…La pena será (… se agrava), en los siguientes casos:

- Cuando las acciones descritas en esta norma, son realizadas por personas encargadas de los soportes; electrónicos, informáticos, magnéticos y telemáticos.
- En el caso de que el encargado del soporte sea un empleado público.
- Si la información vulnerada corresponde a un menor de edad. Abuso en el uso de medios informáticos.

"Será sancionado…, el que sin autorización o cediendo la que se le hubiere concedido, con el fin de procurar un beneficio indebido para si o para un tercero, intercepte, interfiere, use o permita que otra use un sistema o red de computadoras o de telecomunicaciones, un soporte lógico, un programa de computación o de telecomunicaciones, un soporte lógico, un programa de computación o una base de datos, o cualquier otra aplicación informática, de telecomunicaciones o telemática."

El abuso de los medios informáticos, que en realidad no lo tenemos identificado pero que tiene una parte interesante, porque es aquel que sin que le diera la autorización o habiéndola concedido hace que alguien ingrese a un sistema y obtenga un beneficio indebido.

"Será sancionado…, el que sin autorización o cediendo la que se le hubiere concedido, con el fin de procurar un beneficio indebido para si o para un tercero, intercepte, interfiere, use o permita que otra use un sistema o red de computadoras o de telecomunicaciones, un soporte lógico, un programa de computación o de telecomunicaciones, un soporte lógico, un programa de computación o una base de datos, o cualquier otra aplicación informática, de telecomunicaciones o telemática."

Suplantación de identidad: *"Será sancionado…, aquel que utilizando la identidad de otra persona, se haga pasar por esta, en cualquier red social (Facebook, Hi5, MySpace, Twitter, Bebo, etc.)."* Hay otras redes por ahí, pero estas son 4 de las más importantes donde se utiliza mucho la suplantación de identidad y por suerte hoy día eso no tiene sanción.

Hurto Agravado: *"Artículo 209. Se aplicará prisión de…, en los siguientes casos: Si se hiciere uso de ganzúa, llave falsa u otro instrumento semejante, o de la llave verdadera que hubiere sido sustraída, hallada o retenida, claves de acceso o tarjetas magnética."*

El problema con el hurto agravado, es que cuando las tarjetas débito y de crédito que son sustraídas le extraen la billetera les extraen el código de acceso porque tienen la clave pegada a un lado de la tarjeta. Bueno este código de acceso hoy día no tiene sanción legal, porque es la utilización que haría el dueño normalmente para utilizarla. Entonces diríamos: es una estafa. No, no es una estafa porque no ha influido para manipular el sistema ni ha cambiado la clave. Bueno entonces si no es eso es un robo, no, sería hurto agravado si utiliza una ganzúa. Eso es una llave, no es que no se utiliza con llave y por lo tanto la única manera de denominarlo al final es claves de acceso o tarjetas magnéticas, es la única manera de tratar el hurto de este tipo de cosas, porque hoy día la sustracción de esa tarjeta solo implica el costo del plástico, no lo que vale porque eso no existe. Entonces tendría que acusarse por el monto del plástico y como está hoy día la Fiscalía dice eso es baratela y siga caminando y entonces por ahí tendríamos problema.

Estafa (no fraude) Informático. Artículo 216 bis: *"Se impondrá prisión de tres a doce años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya o manipule el ingreso, procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema".*

Este sería estafa y no fraude informático, lo que se le incluye es que "influye" pero este verbo influir se puede confundir un poco, entonces se le puede decir manipular, pero aquí sí pusimos el ingreso con el procesamiento y el resultado. Hay varios momentos en la estafas que se pueden realizar uno es el ingreso, el otro es el procesamiento en que se incluyen los *caballos de troya* ó los *troyanos* que nosotros vemos ahí y el otro es el la salida de la información o el resultado de la información, aquí estaría incluida en el 216 bis como una estafa informática.

Espionaje Informático: *"Se impondrá prisión de… al que se apodere, interfiera, transmita, copie, modifique, destruya, utilice, impida, o recicle datos de valor para el tráfico económico de la industria y el comercio. La pena se aumentará en un tercio si son datos de carácter político, relacionados con la seguridad del Estado".*

El espionaje es: "que se apodere, interfiera, transmita, copie, modifique, destruya, utilice, impida, o recicle datos de valor para el tráfico económico de la industria y el comercio. La pena se aumentará en un tercio si son datos de carácter político, relacionados con la seguridad del Estado". Hemos tenido denuncias en la Sala Tercera donde no se pueden acusar por espionaje porque no tenemos el tipo penal y entonces hay que meterlos por estafa y la cosa se da complicada ahí porque muchas veces la acción no da para meterlos por estafa.

Bueno aquí hay una cuestión interesante con respecto al tráfico económico de la industria y el comercio, existe el caso de un empresa que tenía una fórmula para ofrecer un producto y un empleado disconforme con su jefe logró extraer –porque tenía el acceso para ello- la información científica para producir ese bien y se lo empezó a enviar en partes a la competencia. A la competencia le pareció raro y le dijo sígame enviándome eso porque luego hubo contactos policiales se extrajo la información y luego se le comunico a la misma empresa, todo estaba bajo control, meter esto como espionaje informático sería muy sencillo, pero hoy día tendríamos que meterlo como estafa y es muy complicado.

Uso de virus: *(software malicioso -malware-) "Se impondrá pena de prisión de… al que produzca, trafique, adquiera, distribuya, venda,*

envíe, introduzca o extraiga del territorio nacional virus (software malicioso), u otro programa de computación de efectos dañinos".

Luego el uso de los virus "que se apodere, interfiera, transmita, copie, modifique, destruya, utilice, impida, o recicle datos de valor para el tráfico económico de la industria y el comercio. La pena se aumentará en un tercio si son datos de carácter político, relacionados con la seguridad del Estado".

Clonación de páginas electrónicas (páginas web): *"Se impondrá prisión de…, siempre que no se trate de una conducta sancionada con una pena más grave, al que diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas clonadas de una original previamente existente".*

Clonación de páginas esto es importante porque hoy día la clonación de páginas no tienen ninguna responsabilidad penalmente hablando. Sí hice un clon, sí usted la utiliza indebidamente está cometiendo una conducta delictiva -habría que ubicarlo- pero hoy en día no es un delito.

Suplantación de sitios web para capturar datos personales (Phishing - Pharming): *"Se impondrá pena de prisión de ... al que diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas (web side) clonadas de una original previamente existente, enlaces (links) o ventanas emergentes (pop up), con la finalidad de inducir, convencer a los consumidores o divulgar información personal o financiera, modifique el sistema de resolución de nombres de dominio, lo que hace al usuario ingresar a una IP (dirección electrónica) diferente, en la creencia de que está accediendo su banco u otro sitio personal o de confianza".*

Todo lo que tiene que ver con suplantación de sitios web para *phising y pharming* y la idea es que "al que diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas (web side) clonadas de una original previamente existente, enlaces *(links)* o ventanas emergentes *(pop up)*, con la finalidad de inducir, convencer a los consumidores o divulgar información personal o financiera,

modifique el sistema de resolución de nombres de dominio". Mucho de eso tiene que ver con el mismo pharming que hace que el usuario ingrese a una página diferente a la que cree que esta accesando, bueno esto es parte de una conducta delictiva que no está regulada, deberían regularla, no de esta forma pero deberían regularla.

Daño informático: *"Se impondrá prisión de…, al que por cualquier medio accese, borre, suprima, modifique o inutilice, sin autorización, los datos registrados en una computadora"*. El daño informático que es muy parecido a lo que ya habíamos dicho.

Sabotaje informático: *"Se impondrá pena de prisión de… al que destruya, altere, entorpezca o inutilice un sistema de tratamiento de información, sus partes o componentes lógicos, una base de datos o un sistema informático, o impida, altere, obstaculice o modifique su funcionamiento sin autorización".*

La pena de prisión (…se agravará), en los siguientes casos:

- Como consecuencia de la conducta del autor sobreviniere peligro o daño común. Siempre que la conducta no se encuentre más severamente sancionada.
- Si contienen datos de carácter público.

Finalmente, al sabotaje informático se le han añadido unas agravantes como sería: *"Como consecuencia de la conducta del autor sobreviniere peligro o daño común. Siempre que la conducta no se encuentre más severamente sancionada y Si contienen datos de carácter público".*

El Convenio de Europa sobre ciberdelincuencia

José Francisco Salas Ruiz

Para la exposición de este tema decidí basarme en el Tratado de Budapest de 2001 sobre Ciberdelincuencia y hacer una comparación rápida con la legislación de Costa Rica, para ver si, de acuerdo con el estándar europeo, existe un buen nivel de coincidencia en el tema de delincuencia informática. En lo particular, me parece que nuestra legislación deja mucho que desear.

El objetivo de esta presentación es mostrar algunos de los errores y omisiones de la legislación nacional en el campo de los delitos informáticos, sin pretender llegar a ser exhaustivos. Si bien el tema de los delitos informáticos es aún una materia jurídicamente novedosa aunque de algún desarrollo doctrinal, hemos encontrado que en Costa Rica la legislación penal (no sólo la que contempla el propio Código Penal, sino otras leyes especiales que contienes tipos penales informáticos, según mencionaremos) no mantiene un contenido adecuado para perseguir, prevenir o reprender las conductas lesivas de los delincuentes informáticos.

Más aún, el propio legislador nacional ha cometido yerros importantes a la hora de elaborar y emitir tipos penales, pues no sólo ha promulgado normas que bien podrían tenerse por contradictorias,

sino que ha suprimido inexplicablemente algunas de las pocas existentes. Si bien no deseamos realizar aquí un análisis a fondo de las normas penales existentes en Costa Rica, sí es necesario hacer mención en estas importantes deficiencias legislativas para apoyar nuestra posición de reelaborar las normas penales existentes en la materia, y ajustarlas en particular al Convenio de Europa sobre la Ciberdelincuencia.

De antemano, después de analizar otros temas que tienen íntima relación con los delitos informáticos, concluimos que tanto los tratados internacionales firmados por Costa Rica como los tipos penales existentes en cuanto a pornografía infantil como los delitos que sancionan las infracciones a los derechos de propiedad intelectual tienen suficiente protección en el país, merced a la profusa emisión de normas jurídicas que regulan ambos temas.

Así las cosas, nos limitaremos exclusivamente en los tipos penales existentes tanto en el Código Penal como en la Ley de Administración Financiera y Presupuestos Públicos, con referencias obligatorias al Código Tributario y a la Ley General de Aduanas, cuerpos normativos que también contienen importantes sanciones en sus respectivos campos. Como marco de referencia, utilizaremos la Convención de Europa sobre Ciberdelincuencia de 2001, de manera que los diferentes temas sustantivos de que trata dicho acuerdo internacional puedan guiarnos hacia la uniformidad de normas sancionatorias en nuestro territorio.

Aspectos generales

El Convenio Europeo sobre Convenio Europeo sobre Ciberdelincuencia fue firmado en Budapest el 23 de noviembre de 2001. Actualmente, ha sido ratificado por Albania, Armenia, Bosnia, Albania, Armenia, Bosnia & Herzegovina, Bulgaria, Croacia, Chipre, Dinamarca, Herzegovina, Bulgaria, Croacia, Chipre, Dinamarca, Estonia, Finlandia, Francia, Alemania, Hungría, Estonia, Finlandia, Francia, Alemania, Hungría, a, Islandia, Italia, Letonia, Lituania, Moldavia, Holanda, Islandia, Italia, Letonia, Lituania, Moldavia, Holanda, Noruega, Rumania, Serbia, Eslovaquia, Eslovenia, Noruega, Rumania, Serbia, Eslovaquia, Eslovenia, Macedonia y Ucrania.

Macedonia y Ucrania. Además, ha sido firmado también por los Estados Unidos, Japón, Sudáfrica y Canadá.

En América Latina, si bien a la fecha ningún país se ha adherido a él, tanto Chile como Costa Rica, República Dominicana y México fueron invitados a formar parte. A la fecha, sólo República Dominicana y Argentina parecen estar haciendo esfuerzos específicos por incorporarlo a su legislación interna.

El convenio tiene un aspecto importantísimo que es el de la territorialidad, lo que implica que cualquiera de los países que haya suscrito este Tratado que incurra en un delito informático tendría la posibilidad de perseguirlo. Incluso si los efectos del delito han llegado a nuestro territorio, perfectamente pueden perseguirse aunque el autor no se encuentre aquí. Esto no es algo novedoso porque existe también en los convenios sobre droga donde igualmente se persigue el hecho punible en todos los territorios como sí fuera uno solo, o en el Protocolo a la Convención sobre Derechos del Niño, relativo a la venta de niños, la prostitución infantil y utilización de niños en la pornografía, donde también se da esa posibilidad, dada esta característica de extraterritorialidad en este tipo de delitos, por lo que se hace necesario que se persiga los hechos punibles fuera de las fronteras de nuestro país.

Este convenio tiene además dos bienes jurídicos protegidos que antes no se contemplaban: uno de ellos la protección de la información y el segundo la protección del funcionamiento de un sistema informático.

La idea de emitir un convenio de delitos informáticos no es novedosa. En su momento, en la reunión efectuada en Costa Rica en el año 2000, la representación de Costa Rica propuso la creación de un Convenio Interamericano sobre Delitos Informáticos, por las enormes ventajas que representa la normativa supranacional.

Posteriormente, en el Foro Legislativo en Materia de Delitos Cibernéticos, efectuado en la Ciudad de México y organizado por Organización de Estados Americanos, el Departamento de Estado y la Secretaría de Justicia del Gobierno de los Estados Unidos, a finales de enero y principios de febrero de 2004, se evaluó el desarrollo de la normativa latinoamericana en la materia, llegando a la conclusión de

que el tema de la ciberdelincuencia tenía poco o ningún avance en las legislaciones del continente, salvo contadas excepciones.

En ese foro de conocimiento una vez más se reiteró la necesidad de que los países integrantes del continente americano contasen con un convenio internacional sobre delitos informáticos, tomando en cuenta, entre otros motivos, el fracaso de la solución de leyes-tipo en materia represiva que se quiso implantar en el pasado como solución para las diferentes naciones participantes que deseaban actualizar su legislación. Muestra de ello es que aún existen numerosos países que carecen absolutamente de leyes sobre delitos informáticos y otros que las tienen de manera deficiente o insuficiente, como Chile, Paraguay o Costa Rica. En ese mismo Foro, además, se presentó por primera vez a los países participantes el Convenio sobre Ciberdelincuencia, emitido por el Consejo de Europa. Precisamente, una de las conclusiones a las que se llegó era la posibilidad de suscribir el Convenio europeo.

No obstante, en el año 2008 en Bogota, se volvió a hablar de la posibilidad de un convenio interamericano sobre delitos informáticos, idea que chocó con la oposición de la Secretaría de Justicia de los Estados Unidos, cuyos representantes manifestaron que ya existía un acuerdo mundial sobre la materia, el cual es precisamente el convenio de Europa.

A continuación, veamos una breve confrontación entre el contenido del Convenio de Europa sobre Ciberdelincuencia y las normas penales existentes en Costa Rica.

Definición de conceptos

De acuerdo con el artículo 1 del Convenio sobre Ciberdelincuencia, deben establecerse una serie de conceptos. En este caso, el Acuerdo menciona definiciones sobre lo que debe entenderse por “sistema informático”, “datos informáticos”, “proveedor de servicios” y “datos sobre tráfico”.

Los primero que llama la atención es que no se incluye el concepto de “sistema de información”, sino que sólo se limita a los sistemas

informáticos, esto es, las redes o conexión lógica entre computadoras, en cualquier tipo de plataforma.

La legislación de Costa Rica no contiene tales definiciones. Ello se debe a que no se acostumbra en nuestros Ordenamientos Jurídicos incluir definiciones de cada uno de los conceptos que se utilizarán en la norma. Ello corresponde más a una función de Poder Ejecutivo cuando expresamente se le autoriza a emitir reglamentaciones sobre las leyes aprobadas por la Asamblea Legislativa. Por lo tanto, en los Decretos Ejecutivos sí es común encontrar definiciones de los institutos que se vayan a regular. Ello no obsta para que en la propia ley también se recojan de antemano conceptualizaciones, de acuerdo con la voluntad del legislador. Perfectamente, las definiciones que obran en el Convenio de Europa pueden ser incluidas en la legislación nacional, no sólo para lograr criterios interpretativos sino también como referencias a lo largo del texto.

Igualmente, es posible que esas definiciones sean tomadas en cuenta para que nuestro legislador, en su momento, incluya correctamente ambos tipos de sistemas (informáticos y de información) dentro de la protección normativa, pues no se trata de los mismos conceptos, sino que cada uno de ellos tiene aplicaciones diferentes, sin guardar siquiera relación de jerarquía o de género a especie.

Acceso ilícito

Así se indica en el artículo 2 del Convenio de Europa y se refiere al acceso no autorizado a sistemas informáticos, conducta que puede incluir la intención de obtener datos informáticos.

El artículo 196 bis del Código Penal No.4573 de 4 de mayo de 1970 se refiere a la violación de las comunicaciones electrónicas, con un contenido amplio que procura abarcar cualquier conducta que lesione las comunicaciones íntimas de los ciudadanos.

La pena será de uno a tres años de prisión, si las acciones descritas en el párrafo anterior, son realizadas por personas encargadas de los soportes: electrónicos, informáticos, magnéticos y telemáticos."

En este tipo penal, no se entiende a qué se refiere con soportes electrónicos, informáticos o telemáticos. El único soporte que tiene

sentido real es el soporte magnético. Inexplicablemente se omite la referencia a los soportes ópticos. Por tanto, debería incluirse también en el tipo penal.

Interceptación ilícita

Este literal se encuentra contenido en el artículo 3 del Convenio europeo. Se refiere a la interceptación no autorizada e intencional (dolosa), utilizando medios técnicos, de datos en un sistema informático o de transmisiones no públicas.

La totalidad de los verbos que abarca ese numeral del Convenio de Europa no se hayan recogidas íntegramente en la legislación costarricense.

No obstante, el citado artículo 196 bis del Código Penal sanciona la interceptación o interferencia de datos y otros elementos si son llevados a cabo sin consentimiento del titular de ellos, si se hace con la intención de vulnerar la intimidad o secretos del afectado. Remitimos a él nuevamente para corroborar la existencia de los verbos "interceptar" e "interferir" y "desviar de su destino", en referencia a mensaje, datos e imágenes contenidas en cualquier tipo de soporte, sea este electrónico, informático, magnético o telemático. No obstante, dicho artículo no se denomina tiene la misma denominación contemplada en el Tratado, aunque su contenido sí parece llenar los requisitos que se exigen en el cuerpo normativo internacional.

Por su parte, el artículo 229 bis del Código Penal castiga igualmente el acceso sin autorización a los datos registrados en una computadora:

Se reitera la conclusión anterior en el tanto las acciones sancionadas en dichos tipos penales parecen sujetarse a las exigencias del acuerdo europeo. Por lo tanto, en principio, no se requeriría adicionar más verbos activos, aunque igualmente ello puede ser objeto de revisión, especialmente porque la forma en que están redactadas ciertas conductas podría ser reiterativa, especialmente en lo que se refiere a la acción de borrar datos, contemplada en ambos tipos penales, y con la única diferencia de que en el primer caso la intención debe ser "descubrir los secretos o vulnerar la intimidad de otro"; mientras que en el segundo tipo penal simplemente se exige "falta de autorización", aunque las conductas sean idénticas.

Interferencia en los datos

Registrado en el artículo 4 del Convenio de Europa, la "interferencia en los datos" consiste en conductas que causen daños, borren, deterioren, alteren o supriman datos informáticos en general. Se contempla también la posibilidad de que tales conductas provoquen daños de mayor gravedad.

El artículo 229 bis de nuestro Código Penal, citado en el punto anterior, contiene los verbos "borrar", "suprimir", "modificar" e "inutilizar", sin autorización, los datos registrados en una computadora, por lo que creemos que esta figura se halla debidamente contemplada en nuestra legislación punitiva.

A pesar de lo indicado, pensamos que su redacción podría precisarse aún más, pues su contenido es sumamente genérico. Tomemos en cuenta que no todos los "datos" que se encuentran en una computadora tienen el mismo valor. Quizás debería pormenorizarse según los medios empleados para el borrado, supresión, etc., si es efectuado mediante el empleo de programas dañinos, tales como virus, gusanos, programación, empleo de programas destinados para ello, choque electromagnéticos, etc. Recordemos que los sistemas operativos tienen el borrado y destrucción de datos como una de sus funciones normales, y no todos los elementos eliminados guardan el mismo nivel de importancia, esto es, no es lo mismo eliminar el archivo command.com que los registros de la papelera de reciclaje o los mensajes electrónicos borrados.

Por su parte, y en el mismo sentido del numeral anterior, el artículo 111 de la Ley de Administración Financiera de la República y Presupuestos Públicos N° 8131 de 18 de setiembre de 2001 señala las sanciones contra funcionarios públicos o personas particulares que causen daños a sistemas informáticos de la administración financiera y de proveeduría de las instituciones públicas.

Nótese que la existencia de este artículo es innecesaria pues el sujeto activo puede ser cualquier persona, sean funcionarios públicos o particulares. Además, su redacción carece de técnica legislativa, es confusa y reiterativa, pues sus verbos activos ya se encuentran contemplados en los tipos que recoge el Código Penal, según hemos citado.

Interferencia en el sistema

En el artículo 5 del Convenio está contenida la denominada interferencia en el sistema, la cual se describe como una obstaculización grave, dolosa e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daños, borrado, deterioro, alteración o supresión de datos informáticos.

Una vez más citamos el artículo 229 bis el cual, en sus párrafos finales, contempla sanciones en caso de que, con ocasión de la alteración de datos o sabotaje informático, se entorpeciese o inutilizase una base de datos o sistema informático. Por demás, el mismo artículo, en su párrafo final, dispone la penalización según el resultado lesivo de la conducta.

Así las cosas, parecen cumplirse con las exigencias del Convenio europeo, al menos en cuanto a la protección de los sistemas informáticos, y el agravante de la pena cuando se trate de sistemas de información públicos.

Por su parte, nos permitimos citar el artículo 111 de la Ley de Administración Financiera que, en su inciso b), sanciona la acción lesiva que cause daño no sólo a los sistemas informáticos, sino también a los componentes físicos (aparatos, máquinas o accesorios) que apoyen el funcionamiento del sistema automatizado.

Una vez más, reiteramos la necesidad de revisar en profundidad el contenido de este artículo, pues su redacción es poco técnica y confusa. Por ejemplo, en cuanto al uso de palabras como "dolosamente", la cual resulta reiterativa pues se entiende que todo tipo penal se reputa doloso a menos que el legislador cree un tipo culposo, situación que no ocurre en este ni en ningún caso.

Abuso de los dispositivos

Sanciona la tenencia, producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de programas de cómputo o similares que sirvan para el acceso, intercepción, interferencia de datos o de sistemas informáticos (incluyendo las conductas vistas arriba: destrucción, inutilización, alteración,

etc.) o bien, contraseñas, códigos de acceso o datos informáticos o similares que permitan acceder a un sistema informático. En el caso de la creación o tenencia de dispositivos tales, el propio convenio prevé la posibilidad de que se exima de responsabilidad la conducta si los programas de cómputo no han sido creados originalmente para fines ilícitos.

No existe en Costa Rica una disposición similar. Se hace necesaria su creación legislativa expresa y que su contenido tenga alcances generales.

Más aún, el delito denominado "suplantación de personalidad" tampoco se encuentra contemplado en la legislación nacional, en cuanto al uso ilegítimo de nombres de usuario y claves de acceso para acceder a sistemas de información. En realidad, disposiciones que penan tal conducta se encuentran previstas apenas en materia aduanera y tributaria, legislación que puede servir de ejemplo para crear otros tipos penales de carácter general que ayuden a complementar la legislación existente.

Estafa informática

Por su parte, la estafa informática, según el artículo octavo del Convenio, consistiría en la introducción, alteración, borrado o supresión de datos informáticos, o la interferencia en el funcionamiento de un sistema informático, con el objeto de obtener ilícitamente un beneficio económico ilegítimo para sí o para un tercero.

El Código Penal de Costa Rica, según hemos ya mencionado en su momento, contempla, con esos mismos términos, la alteración de datos y el sabotaje informático, en el cuestionado artículo 229 bis, y sanciona el acceso, borrado, supresión, modificación o inutilización no autorizada de datos registrados en una computadora. Añade mayor pena si con el actuar ilícito se entorpece o inutiliza además un programa de cómputo, base de datos o sistema informático. Como detalle adicional, la pena se eleva aún más si el ataque es cometido contra sistemas de información de naturaleza pública.

Los problemas de redacción que presenta este artículo son variados. En primer lugar, su denominación no es igual a la del Convenio, el

cual denomina a esas figuras como “estafa informática”, mientras que en el Código Penal de Costa Rica se conocen como “alteración de datos y sabotaje informático”.

Además, por una parte, no es clara la diferencia entre base de datos y un sistema de información, término que se echa de menos en él. Confunde el concepto de sistema informático con el sistema de información, el cual no protege. Igualmente, la utilización de los verbos es confusa pues, en el caso de un programa de cómputo, su entorpecimiento es fácil, por lo que podría ser efectuado por cualquier persona, sin indicar el medio. Tampoco señala mayor penalidad por el resultado producto del hecho punible.

Falsedad informática

En este artículo se incluye un delito informático de gran relevancia, como es la falsificación informática. Según los términos del Convenio sometido a consulta, la falsificación informática incluye la introducción, alteración, borrado o supresión de datos informáticos con la intención de que se tengan como auténticos para cualquier efecto legal.

En tal sentido, el Código Penal costarricense fue reformado para incluir normas que sancionen esas conductas, en el artículo 217 bis:

El primer punto en que existe discordancia es en la denominación del tipo penal, pues el Convenio Europeo denomina a dichas conductas como “falsedad informática” mientras que en el Código Penal de Costa Rica se le llama “Fraude Informático”.

Si bien los términos de este artículo son bastante criticables, al no incluir los componentes de entrada ni hacer énfasis en la noción del concepto básico de “sistema” (entrada, procesamiento, salida), sí parece cumplir, al menos, con el requisito exigido en el Convenio europeo. No obstante, de la redacción, bastante criticable, parece exigirse que el resultado del hecho delictivo se produzca en el procesamiento (caja negra) del sistema, y no en su salida, lo que exige una revisión y reelaboración del tipo penal.

Responsabilidad de las personas jurídicas

No existe legislación en nuestro país que castigue a las personas jurídicas de la forma como lo desease el Convenio, dado que las

sanciones se dirigen siempre contra personas físicas y no morales. Sólo en el plano de la responsabilidad civil podría pensarse en sancionar a una persona jurídica, pero es poco probable que se modifique alguna norma para exigir responsabilidad penal a una persona jurídica.

Conservación rápida de datos informáticos almacenados

Tampoco existe legislación expresa, en materia procesal penal, que trate expresamente de la conservación de datos informáticos. De hecho, no existe norma alguna que obligue de oficio a los denominados ISP's o proveedores de servicios de Internet a conservar algún dato almacenado por sus usuarios. La única manera como ello podría ocurrir es en virtud de una orden judicial, emanada por juez competente dentro del marco de una investigación abierta. Propiamente dentro de la investigación, se da la intervención de la Unidad de Delitos Informáticos del Organismo de Investigación Judicial, dependiente del Ministerio Público, a su vez órgano del Poder Judicial. Es tal unidad técnica de investigación la que puede lograr capturar, almacenar, conservar y poner a disposición del juez o fiscales los datos informáticos que se recaben a lo largo del proceso investigativo. No se regula de manera expresa, sino que habría que recurrir a las normas de aplicación general del Proceso Penal.

Ausencia de tipos penales

En Costa Rica ciertas conductas no se encuentran tipificadas, tales como el espionaje informático, el *phishing, pharming*, la suplantación de personalidad, la protección de datos personales, difusión de virus, suplantación de páginas o sitios web, al igual que la facilitación del nombre de usuario y clave de acceso a sistemas públicos (las cuales sólo se dan en legislación aduanera y tributaria). También debe hacerse una separación de las conductas y no concentrarlas todas en un mismo tipo penal. Deben eliminarse algunos tipos penales innecesarios.

En suma, con base en los ejemplos vistos, es posible darse una idea del panorama legislativo actual en Costa Rica en materia de delitos informáticos, el cual requiere de un análisis profundo por parte del legislador para solventar muchísimas carencias y normas incompletas.

Capítulo 5
Prevención y sanción de los ciberdelitos

La ingeniería social

Erick Lewis Hernández

La mayoría de fraudes informáticos se basan en la ingeniería social que es la ciencia de manipular a las personas para obtener información confidencial, por lo general va a atacar al humano, muchas veces nos imaginamos a un *hacker* que trata y trata de entrar información técnica que le permita realizar un ataque más sencillo que le permita ahorrar tiempo.

Por lo general busca la confianza de la gente, por ejemplo el *phising*, que es un correo electrónico que viene del banco y dice que hay un problema de seguridad, que nos da confianza pero a la vez nos amenaza, si en 24 horas no actualiza sus datos le cerramos su cuenta. Eso es fraude porque nos da confianza pero a la vez nos presiona.

El delincuente piensa como reaccionaría la mayoría de personas ante una situación: Utiliza llamadas telefónicas, SMS, correos electrónicos, redes sociales, sistemas de mensajería. No hay tecnología capaz de proteger un sistema contra la Ingeniería Social.

En estos casos en general, en la ingeniería social el delincuente piensa y anticipa la reacción de la gente para hacerlos caer más fácil, utiliza llamadas telefónicas, correos electrónicos, mensajes de texto, redes sociales, en realidad cualquier medo de comunicación.

No hay tecnología capaz de proteger un sistema contra la ingeniería social, realmente como les digo nosotros no sabemos decir que no, si nos alaban, si se nos presenta una persona en la oficina a decirnos que bonitos vinimos hoy, que bonito somos, nos abrimos y ya le damos información que no deberíamos darle y esto se presta no solo en los fraudes informáticos sino en cualquier ámbito de nuestra cultura.

Programa espía *(Keylogger)*

- Es un programa muy pequeño que se instala en la computadora del objetivo.
- Se ejecuta sin que el usuario se dé cuenta.
- No presenta signos visibles.
- Guarda cada tecla presionada en el teclado.
- Envía la información recopilada por correo electrónico o FTP.

Es un programa muy pequeño que se instala en la computadora se ejecuta sin que el usuario se de cuenta, no presenta signos visibles, no tiene iconos, no tiene nada. Guarda cada tecla que ustedes pulsen en el teclado y una vez que la guarda la envía por correo electrónico o FTP que es un protocolo que permite enviar archivos electrónicos, al delincuente y ya tienen acceso.

El delincuente lo que hace es que envía un correo masivo.No se esta teniendo un ataque a cierta persona individual o a cierto grupo, se hace masivo, tenemos denuncias no solo en este caso sino también en el de *phising* que ahora vamos a ver de personas que le sacaron desde 50 mil colones, 300 mil, 1 millón de colones, tenemos un caso que yo creo que es el pico de 240 mil dólares que en 15 días lo sacaron, la gama es muy variada.

Ese correo electrónico lleva un archivo en ese momento se utilizaban temas como el TLC, ese archivo lleva el programa escondido, a la hora que usted abre el archivo la computadora se le infecta, el programita

empieza a guardar todo lo que usted esta digitando sea un texto, una carta, o cuando se esta entrando al banco -en realidad lo que le interesa al delincuente- y envía los datos al delincuente.

Ya una vez con esto el delincuente ya tiene personas que están buscando cuentas para trasladarle los dineros y poderlos extraer del banco, muchas veces en tiempos rápidos, tenemos casos que en 15 minutos ya han sacado la plata del banco, pareciera que la persona que iba a sacarlo ya estaba haciendo fila en el cajero o en la caja.

Phishing

Es una estafa o fraude que utilizando medios informáticos o electrónicos e ingeniería social, tiene como fin extraer información confidencial de sus victimas y utilizarla para extraer dinero u otros fines. Para esto se hace pasar por una persona o empresa que requiere su información confidencial.

El *Phising* es una estafa o fraude que utiliza medios informáticos o electrónicos e ingeniería social, tiene como fin extraer información confidencial de sus victimas y utilizarla para extraer dinero u otros fines, para extraer cuentas de correo electrónico En realidad hemos tenido casos más caseros donde una persona tenía una relación con otra y quería ingresar a su cuenta de correo electrónico, mandó un supuesto correo de Yahoo, se lo mando bastante casero pero desgraciadamente la gente solo se fija en los logos, le dice que por favor le brinde el usuario y la contraseña esta persona cayó y pudo ingresar.

Este es un ejemplo más gráfico, usan la página del Banco de Costa Rica mandan un correo electrónico con los logos del banco para que de un poco de confianza. Los usuarios del BCR para ingresar al banco han activado los parámetros, la activación será de inmediatamente en línea, donde contactará a nuestro equipo de seguridad y ahí sigue. Todo esto para ingresar a la página del Banco pero en realidad lo redirecciona a un sitio que se publica por lo general en sitios gratuitos no en Costa Rica, tal vez en China, en Rusia y la activan durante cierto tiempo realmente la montan un cierto tiempo la sacan de línea y ahí van.

En general este te pide la clave y el usuario y en la parte de acá dice que nunca revele sus datos por medio de correo electrónico que el banco nunca se los va a pedir, pero la gente se enfoca en lo que quiere.

Pharming

- Técnica basada en la Ingeniería Social, que data del año 2004.
- Correo electrónico con un enlace hacia un sitio con información de su interés.

Estos delitos informáticos están evolucionando en cuánto más trabas le ponga el banco, más van evolucionando. Por ejemplo el Banco de Costa Rica decidió proteger a sus clientes a través de una tarjetita con un montón de números, la clave dinámica y entonces están recurriendo a una técnica que se llama *pharming.* Es una técnica igualmente basada en la ingeniería social, lo que se hace es que se envía un correo electrónico que tiene un enlace a un sitio con información de interés.

Con el *pharming* la víctima siempre es conducida al sitio falso del banco, aunque digite correctamente la URL. El supuesto sitio del banco solicita información adicional a la víctima. Y la computadora o enrutador de la víctima sufre cambios en su configuración.

La victima siempre es conducida a un sitio falso, es igual que *phising,* se le solicita la información, la diferencia es que la computadora del ofendido o el enrutador del computador que es el aparatito donde llega la conexión de Internet puede ser vulnerado. Tenemos dos variantes nos pueden cambiar alguna configuración en la computadora o nos cambian la configuración del aparatito de Internet que tenemos en la casa.

¿Para qué? Hay algunas técnicas que puedan afectar incluso algunos servidores de RACSA, del ICE o de cualquier otra empresa que preste servicios de acceso a Internet puedo mandar a varias personas masivamente para que podamos cometer un error y entrar con datos falsos.

Este sitio se llama el *gusanito.com* que utilizaban estos delincuentes para hacer *Pharmig*, gusanito es una página que dan tarjetas virtuales de cumpleaños y de felicitación gratuitas y normalmente cuando a mi me mandan una invitación de estas dice: fulano de tal le envío una tarjeta de felicitaciones y haga click aquí para ver su tarjeta.

Aquí se puede ver donde dice ha recibido una tarjeta especialmente para ti, en nuestro sitio, para verla haz click en el enlace y descarga nuestra nueva herramienta. Te esta diciendo descargue una herramienta y la gente está diciendo yo quiero ver la tarjeta ese es mi fin el resto no importa.

Lo que hace es descargar esa herramienta se ejecuta un procedimiento ahí y lo que hace es que este archivito que se llama Host es un programita que nos permite a los informáticos en una computadora que cuando hay varias redes o ciertas situaciones poder enrutar o visualizar la información que queremos lo que hace es agregar esta modificación que se pega a una conexión IP, que una dirección IP es un numerito que identifica a todas las computadoras a nivel mundial que están en Internet en una red.

En este caso usted digita en una computadora www.yahoo.com pero en realidad esto es una máscara detrás de ese yahoo.com, en realidad lo que hay es una dirección IP, pero para efectos prácticos es más fácil aprenderse yahoo.com que ese montón de numeritos, veamos eso con lo teléfonos celulares ya no nos aprendemos los números ahora los buscamos en la agenda.

Básicamente algo que se descargó para visualizar la tarjeta, cuando la persona va a entrar lícitamente al banco, digita banco.com, para no hablar de ningún banco básicamente él antes de irse a Internet le dice revise este archivo donde vea que la persona digito lícitamente y que la persona esta confiada de que tiene un link y desgraciadamente lo redirecciona a un sitio falso.

Por ejemplo hablamos con policías de Brasil, ellos al mes reciben 400 denuncias de estos delitos que hemos hablado de *phising* y de *pharming*, desgraciadamente como hemos hablado este tipo de delitos son difíciles de perseguir por lo general parte de la banda

esta aquí, y la otra parte de la banda esta fuera de Costa Rica esto es muy normal.

Los policías de la guardia civil de España nos cuentan que muchas de las bandas están ubicadas propiamente en los países bajos de Europa y lo que tienen meramente es la parte operativa en España y los dineros son transferidos al extranjero.

Este es más o menos el modo de operar del *pharming* el delincuente envía un correo electrónico a la victima igual es un correo masivo, no es para una persona, igual la persona abre la postal falsa le modifica la configuración de la computadora, cuando la persona ingresa lícitamente supuestamente a su banco lo remite a un sitio falso ahí entra sus datos que son enviados al delincuente, el delincuente entra lícitamente al sitio verdadero del banco y ya con la información del usuario y de la clave dinámica de la victima, transfiere el dinero a frenteadores y reclutadores, los reclutadores son las personas que buscan cuentas o que tienen cuentas, y los frenteadores son los llamados mulas que van a las ventanillas o al cajero automático a retirar el dinero y en algunos casos obtienen una comisión, en algunos casos en otros ni si quiera saben, retiran el dinero y el dinero va a dar a los delincuentes.

Violación de las comunicaciones electrónicas

- Un administrador de correos electrónicos de una institución pública, creó una regla que le reenviaba los correos de varias cuentas de correo.
- Muchos casos en que a la persona le roban la contraseña de su correo personal y accesan a información confidencial y personal.

Por ejemplo un administrador de correos en una institución pública creó una regla que le reenviaba a sus compañeros de trabajo y al jefe, cada vez que le llegaba un correo electrónico al jefe se lo reenviaba a él.

Dentro de lo que es también la violación de las telecomunicaciones electrónicas llegan muchas denuncias de gente que dicen que alguien a través de un medio electrónico esta ingresando a su correo

electrónico y esta enviando información que tenía ahí a terceras personas, esto puede ser con fines amorosos desgraciadamente hay relaciones amorosas que no son muy normales o que no deberían de ser y muchas veces reenvían correos electrónicos personales, muchas veces se hace como broma, muchas veces se hace para ingresar a información confidencial.

Modos de operar en Costa Rica

- Alteración de datos y sabotaje informático. Lo que es sabotaje y alteración de datos que es otra forma que el código penal identifica.
- Acceso a sistemas de entidades públicas.
- Venta de información confidencial a través de correo electrónico.
- Daño de datos en equipos personales.
- Cambio de saldo en cuentas bancarias.

Básicamente lo que hace es un entrar a un sistema de una entidad pública, hubo el caso de una persona que tenía impedimento de salida. Técnicamente había una persona que alteraba la base de datos de migración quitaba el impedimento de salida, la persona salía del país y esta persona volvía a restaurar la base de datos, por lo que no coincidía porque salió con el impedimento de salida.

También venta de información confidencial a través de correo electrónico donde gerentes de empresas recibe un correo yo tengo un montón de formulas de cierta empresa que es la competencia, yo puedo vendérsela a cierto precio y por cierto tiempo, este gerente en realidad no quiso seguir con esto, llamó al gerente de la compañía ofendida ellos pusieron la denuncia y se le dio seguimiento se identifico que esos correos salían de la empresa ofendida se empezó a realizar una investigación informática se identifico un usuario que ingresaba a Yahoo a las horas que más o menos se enviaban los correos electrónicos y resulta que se determino por otros medios que no era ese usuario sino que era un subalterno que conocía la clave de él y probado que era él se pudo iniciar un proceso policial y se pudo condenar a 6 años a esta persona.

Se han dado algunos casos donde se daña el equipo personal, cuando despiden a alguna persona y le dan chance de sacar su información personal y daña los equipos. También hay algunos casos que se han dado en empresas bancarias en tres ocasiones hay un informático que alteraba los saldos de su cuenta bancaria arreglaba un poco los números, lamentablemente la denuncia se puso en el 2001 no se logró probar nada no habían rastros, no habían pistas, evidencia informática por falta de controles.

Otros delitos/ evolución nuevos delitos

- Producción de Pornografía Infantil
- Difusión de Pornografía Infantil
- *Child Grooming:* Acoso infantil a través de programas de conversación y coaccion al menor con fotos o videos comprometedores. Aquí otros delitos que se cometen a través de medios informáticos.

La producción de pornografía infantil que algunos expertos dicen que es un delito informático, a mi criterio no sí la informática ha facilitado mucho la comisión de estos delitos principalmente lo que es la pornografía.

Hay otras formas de ataques que afectan también a los niños como lo es *Child Grooming* que es el acoso de los niños a través de *chat*, de sitios de conversación. Hay un caso de una menor que esta chateando recibe la invitación de otra persona que quiere hablar, están hablando cuando llegó a ganar la confianza le dice que él conoce donde vive y quienes son sus papás que si no se desnuda y le muestra sus partes íntimas a través del *Web Cam* va a ir a matar a los papás, desgraciadamente la menor accede se quita la ropa, al día siguiente la persona le envía un correo electrónico diciendo vea yo tengo sus fotografías, sus videos tengo el correo electrónico de su papá, de su mamá, sino lo hacemos otra vez a tal hora le voy a enviar eso a sus papás.

La niña lo denunció, resulta que era una persona del Salvador que revisando en su HI5 tenía más de 2000 amigas que eran niñitas entre

10 y 15 años de toda Latinoamérica, en uno de los comentarios de esas niñas de Honduras le dice que ojala nos volvamos a ver y pone una foto con él besándose, trasciende de un país a otro.

Robo de identidad

- Utilización de información publicada en redes sociales.
- Utilización de fotografías.
- Búsqueda de información publicada en Internet.

El robo de identidad que se hace a través de información que publicamos en HI5 y en todas estas redes sociales se da mucho y se va a dar cada día más.

Amenazas y extorsiones

- Utilización de correos electrónicos.
- Envío de mensajes de texto desde páginas web que brindan este servicio.

A través del correo electrónico se hacen amenazas, extorsiones, incluso secuestros ya no se envían cartas, se envían correos electrónicos.

Estafas y fraudes

- *Carding:* es un derivado del *phishing* para obtener números de tarjetas de crédito y realizar compras en Internet.
- Tecnificación.
- Uso de páginas web falsas.
- Correos electrónicos fraudulentos (*Estafa nigeriana*)

Han tecnificado las estafas y fraudes, ya lo que es el robo de tarjetas se hace a través de Internet, o de esquivas, usted va a una bomba paga le da la tarjeta al dependiente, la pasa por la máquina y ya le robaron toda la información.

Bulling (acoso escolar)

- Maltrato físico o Psicológico entre menores
- Uso de correo electrónico
- Redes sociales

El *Bulling* es el acoso escolar que en nuestro país se da en una proporción menor pero a eso vamos, que consiste en el maltrato físico y psicológico ahora se utiliza medios electrónicos para maximizar ese abuso.

Cyberterrorismo

- Terrorismo + Internet
- Infundir temor
- Utiliza medios masivos como Internet
- Utiliza el encriptamiento de sus propios correos electrónicos
- Potenciales ataques terroristas a través de las redes
- Sistemas de navegación
- Sistemas financieros
- Alteración de formulas químicas

El cyber terrorismo esta bien utilizado por algunos organizaciones para difundir el mensaje, inclusive se pueden dar ataques terroristas a algunos sistemas vitales de algunos países.

Algunas experiencias de los delitos en línea

Adriana Rojas Rivero

Algunas experiencias con el tema de los delitos en línea, con relación a la responsabilidad civil indemnizatoria. Se han formulado diferentes denominaciones para indicar las conductas ilícitas en las que se usa a la computadora, tales como "delitos informáticos", "delitos electrónicos", "fraude cibernético", "fraude informático", entre otros.

Los delitos informáticos surgen a raíz del uso indebido de las computadoras y de cualquier medio informático, susceptibles de ser sancionadas por el derecho administrativo, civil y penal.

Todos los sistemas informáticos son vulnerables de ser atacados por personas expertas en computación, con intenciones delictivas, tales como la obtención de datos personales incluidos en medios informáticos, estafas, fraudes, ventas ilegales por internet, comercialización por internet de pornografía infantil; plagios de obras musicales, literarias o cinematográficas para vender las reproducciones, entre otros.

La primera característica de esta nueva modalidad de fraude es el robo de información y con ello el uso de la falsa identidad virtual.

Modalidades

a.- *Phishing* (pesca de contraseñas)

Fases:

- En la primera fase, la red de delincuentes se nutre de usuarios de chat, foros o correos electrónicos, a través de mensajes de ofertas de empleo con una gran rentabilidad o disposición de dinero (hoax o scam). En el caso de que caigan en la trampa, los presuntos intermediarios del delito, deben rellenar determinados campos, tales como datos personales y número de cuenta bancaria.
- En la segunda fase, se comete el *phishing*, ya sea el envío global de millones de correos electrónicos bajo la aparien cia de entidades bancarias, solicitando las claves de la cuenta bancaria (*Phishing*) o con ataques específicos.
- El tercer paso consiste en que los delincuentes comienzan a retirar sumas importantes de dinero, las cuales son trans mitidas a las cuentas de los intermediarios (son denomina dos muleros o burros).
- Por último, los intermediarios realizan el traspaso a las cuentas de los ladrones, llevándose éstos las cantidades de dinero y aquéllos —los intermediarios— el porcentaje de la comisión.
- Distinguir un mensaje de phishing de otro legítimo resulta muy difícil para el cliente, ya que para el delincuente es muy fácil modificar la dirección de origen que se muestra.

b- Troyanos

Se denomina troyano o caballo de Troya a un programa malicioso capaz de alojarse en computadoras y permitir el acceso a usuarios externos, a través de una red local o de Internet, con el fin de recabar información o controlar remotamente a la máquina anfitriona. http://es.wikipedia.org/wiki/Caballo_de_Troya_(inform%C3%A1tica).

Habitualmente se utiliza para espiar, usando la técnica para instalar un software de acceso remoto que permite monitorizar lo que el

usuario legítimo de la computadora hace (en este caso el troyano es un spyware o programa espía) y, por ejemplo, capturar las pulsaciones del teclado con el fin de obtener contraseñas (cuando un troyano hace esto se le cataloga de keylogger) u otra información sensible.

La mejor defensa contra los troyanos es no ejecutar nada de lo cual se desconozca el origen y mantener software antivirus actualizado; es recomendable también instalar algún software anti- troyano, de los cuales existen versiones gratis aunque muchas de ellas constituyen a su vez un troyano. Otra solución bastante eficaz contra los troyanos es tener instalado un *firewall*.

Otra manera de detectarlos es inspeccionando frecuentemente la lista de procesos activos en memoria en busca de elementos extraños, vigilar accesos a disco innecesarios, etc.

Lo peor de todo es que últimamente los troyanos están siendo diseñados de tal manera que, es imposible poder detectarlos excepto por programas que a su vez contienen otro tipo de troyano, inclusive y aunque no confirmado, existen troyanos dentro de los programas para poder saber cuál es el tipo de uso que se les da y poder sacar mejores herramientas al mercado llamados también “troyanos sociales”.

Algunos ejemplos de los efectos de los troyanos son:

- Borrar o sobreescribir datos en un equipo infectado.
- Espiar y recolectar información sobre un usuario y enviar de incógnito los datos, como preferencias de navegación y estadísticas a otras personas.
- Tomar capturas de pantalla en determinados momentos para saber lo que está viendo el usuario y así capaz detectar las contraseñas que se escriben en los teclados virtuales.
- Monitorizar las pulsaciones de teclas para robar información, nombres de usuario, contraseñas o números de tarjetas de crédito *(keyloggers*).
- Engañar al usuario mediante ingeniería social para conseguir sus datos y números bancarios y otros datos de su cuenta que pueden ser usados para propósitos delictivos.

c- Hombre en el Medio *(man in the middle*)

Es un ataque en el que el enemigo adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado. El atacante debe ser capaz de observar e interceptar mensajes entre las dos víctimas. http://es.wikipedia.org/wiki/Ataque_Man-in-the-middle.

La posibilidad de un ataque de hombre en el medio sigue siendo un problema potencial de seguridad serio, incluso para muchos criptosistemas basados en clave secreta.

Casos conocidos de fraude informático

Instituciones públicas: Caso INS

En el año 2006, hubo un proceso penal por fraude informático, contra un empleado de la institución, que junto con varias personas, se organizaron para el cometer el fraude.

El funcionario ocupaba el puesto de oficial de público, al cual entre otras cosas, le correspondía la atención del público en las rehabilitaciones de pólizas, cambio de beneficiarios en los seguros de vida, etc.

Este señor empezó a realizar el trámite masivo de rehabilitación de pólizas de vida, lo cual consiste en rehabilitar la póliza que se había cancelado por falta de pago. Ej: se cancela el seguro de vida porque no continuó pagando el titular de la misma, la cual se puede rehabilitar únicamente cuando el titular continúa pagando la misma.

Las pólizas de vida individual ofrecen el servicio de préstamo de dinero sin fiador, porque la garantía es la misma póliza. El procedimiento para solicitar el dinero es personal o por medio de apoderado.

El funcionario del INS, rehabilitó cientos de pólizas individuales de vida, por medio de apoderados, quienes eran las personas con quien se asoció, de tal suerte que el INS les entregaba el dinero al supuesto apoderado y éste compartía la ganancia con el funcionario público.

La pérdida económica para el INS fue de 264.000.000 de colones, en el año 2004.

Fraudes bancarios: cuentas bancarias y tarjetas.

Cuentas bancarias

Una vez robada la información de datos y la identidad virtual, el fraude consiste en la sustracción ilegítima de dinero de una cuenta bancaria, por medio de internet.

Los fraudes cibernéticos están siendo realizados por un grupo de delincuentes bien organizados y estructurados, con suficiente personal experto en computación. Se trata sin duda alguna, de una modalidad de crimen organizado internacional.

Este grupo de delincuentes, de forma ilegítima roba la información de un grupo de personas para tener conocimiento de los servicios que la banca le ofrece al cliente, de los números de cuenta, de los PIN o PASSWORD, de la cantidad de dinero y los movimientos que hace cada uno de los usuarios de la banca, de los movimientos con tarjetas de créditos y débitos, por lo que se encarga de encontrar la manera de cometer el fraude, y de engañar tanto a la entidad bancaria como a los usuarios, sobre la forma en que es cometido el fraude.

Compras por internet en tarjetas de crédito o débito

Una vez robada la información e identidad virtual, el ladrón virtual procede a realizar compras por medio de internet.

Engaños a empresarios:

Tenemos varios casos como el de un señor, que tiene más de 30 años de ser dueño de siete negocios, entre los cuales se puede mencionar fábrica de persianas, damascos, restaurantes, cabinas y hoteles.

En los 7 negocios, tenía el sistema de cobro por medio de tarjeta de crédito o débito, por internet o de forma física. Desde Nigeria (la cuna del fraude virtual), una "supuesta agencia de viajes" le solicitó para el hotel una reservación de 40 habitaciones, para extranjeros nigerianos y una comisión. En el hotel proceden a realizar las reservaciones, pagan por medio de tarjeta por internet, credomatic le da el visto bueno a los bouchers, ordena el depósito, por lo que el encargado de reservaciones manda la orden de pagar la comisión a la agencia de viajes de Nigeria, por medio de Western Union.

Un mes después, Credomatic llama al dueño del hotel, le pide la reintegración del dinero y lo tilda de estafador virtual, porque hubo fraude por internet, y como sanción, le quita la posibilidad de continuar cobrando con tarjetas en los 7 negocios.

La prevención de estos delitos, es difícil más no imposible. Los grados de seguridad se pueden mejorar, tanto por parte de las instituciones públicas, entidades bancarias y empresarios. Para lo cual se requiere el apoyo de universidades y centros educativos, que enseñen mecanismos para disminuir riesgos, como lo ha hecho Armando Novoa en los talleres de Seguridad Informática en México, con el apoyo de Microsoft e INCECAT de Costa Rica.

Los tipos de responsabilidad por esta conducta, es penal con sanción punitiva en el caso que se logre individualizar al delincuente, administrativa con sanción de multa para el Estado, en caso que se logre demostrar la vulneración del derecho de seguridad de los consumidores y civil con sanción indemnizatoria, por responsabilidad objetiva, al amparo del artículo 35 de la Ley de la Competencia y Defensa Efectiva del Consumidor.

Pero más que prevenciones y sanciones, me gustaría recomendar soluciones. En la Unión Europea, la solución fue el seguro por fraude informático, que en nuestro país no existe a la fecha, dejándonos en un estado total de desprotección.

No hemos podido combatir el robo de vehículos en los últimos 25 años, pero nos sentimos tranquilos con el seguro. Combatir el robo virtual es una misión casi imposible, pero protegernos con el seguro virtual, es mucho más factible.

Delitos de Propiedad Intelectual en el Ciberespacio

Georgina García Rojas

Este artículo abordará los siguientes temas: la protección penal de los derechos derivados de la propiedad intelectual, concretamente los derechos de autor y derechos conexos, las reformas legislativas en esta materia; el análisis de algunas figuras delictivas, los problemas de aplicación de las normas y los retos de la protección de estos bienes en el entorno digital.

Es importante señalar que la obligación de establecer figuras penales y sus correspondientes penas (sea de prisión o pecuniarias) contra delitos tales como la falsificación dolosa de marcas y la piratería lesiva del derecho de autor y derechos conexos, se deriva de diversos tratados e instrumentos internacionales de los cuales Costa Rica forma parte, tales como el ADPIC y el CAFTA-RD.

En ese sentido, el Anexo 1-C, denominado "Aspectos de los Derechos de Propiedad Intelectual y el Comercio" (ADPIC), de la Organización Mundial de Comercio (OMC), aprobado por Costa Rica

mediante Ley Nº7475 de 20 de diciembre de 1994, (Aprobación del Acta Final en que se incorporan los resultados de la Ronda de Uruguay de negociaciones Comerciales Multilaterales).

La norma del ADPIC que determina los procedimientos penales (artículo 61) es muy explícita y exigente, ya que establece la obligación, por parte de los Estados miembros, de implementar *«procedimientos y sanciones penales al menos para los casos de falsificación dolosa de marcas de fábrica o de comercio o de piratería lesiva del derecho de autor a escala comercial».* Incluso determina que, dentro de esos procedimientos y sanciones, se incluirá la pena de prisión o la imposición de sanciones pecuniarias suficientemente disuasorias y coherentes con el nivel de las aplicadas por delitos igualmente graves; además, que cuando proceda existirá también la confiscación, el decomiso y la destrucción de las mercancías infractoras y de todos los materiales y accesorios utilizados predominantemente para la comisión de los delitos. Termina ese artículo diciendo que *«los Miembros podrán prever la aplicación de procedimientos y sanciones penales en otros casos de infracción de derechos de propiedad intelectual, en particular cuando se comenta con dolo y a escala comercial».*

Por otra parte, la Ley Nº 8622, que aprueba el Tratado de Libre Comercio entre Republica Dominicana, Centroamérica y Estados Unidos[1], en su Capítulo XV: Propiedad Intelectual, Artículo 11.- Observancia, en materia de delitos en Propiedad Intelectual, establece la necesidad de combatir *falsificación dolosa de marcas o de piratería lesiva de derecho de autor o derechos conexos a escala comercial* y procura que los países realicen actividad legislativa en ese sentido. Igualmente la importación y exportación de mercancía "pirateada" debe ser considerada igualmente delictiva. La acción del Estado desde la perspectiva penal se espera, por supuesto, tenga efectos disuasorios de futuras acciones reiterativas de los delitos contemplados en la legislación especial.

1 Publicada el 21 de Diciembre de 2007, Gaceta Nº 24.

Costa Rica ya había iniciado la incorporación de estas y otras figuras penales en su legislación, incluso antes del año 2000, sobre todo en materia de derechos de autor y derechos conexos.

Las nuevas tecnologías de la información, que han revolucionado la vida de la sociedad contemporánea gracias a un cambio en el acceso a la información y su procesamiento, también han presentado nuevos retos para los derechos de autor, pues mientras todos contamos con mayor acceso a los distintos tipos de obras, la técnica posibilita actuar en lesión de la propiedad intelectual con mucha facilidad. Sin embargo, también se hacen esfuerzos para que exista coordinación entre tecnología y derechos de autor.

El abaratamiento de las tecnologías de información y comunicación, la disponibilidad creciente de accesos gratuitos a Internet, el aumento de las velocidades de conexión, la ubicuidad de los servicios de interconexión provocada para la integración de las tecnologías telefónicas celulares y la Internet, ha llevado a que la consulta, análisis y diversión con las fuentes disponibles en la Web sea cada vez más intensa, cotidiana y relevante para los ciudadanos.

Junto a lo anterior, debe indicarse que el proceso mismo de globalización de los contenidos ha puesto en verdadera situación de peligro los derechos autorales en Internet, provocando diversos riesgos y peligros que deben ser atendidos por los legisladores de todo el mundo.

Por ejemplo, recientemente ha sido noticia la creación de sitios web en los cuáles se pueden acceder a textos completos de libros, pero para no violentar los derechos de persona alguna, pues se difunden únicamente libros de dominio público, clásicos que pueden ser descargados en forma gratuita. Se impulsa entonces el concepto de una biblioteca electrónica mundial. El llamado “Archivo de Internet”, una biblioteca digital de sitios online, está colaborando con la biblioteca del Congreso de Estados Unidos y otras instituciones para escanear libros y convertirlos en formato digital para computadoras, y cuyo proyecto más reciente es la llamada biblioteca ambulante

online, que puede imprimir más de 100.000 libros antiguos que ya no están protegidos por los derechos de autor, textos cuyas ediciones están casi siempre agotadas.

También existen otros sitios de Internet de búsqueda de un amplio rango de libros electrónicos gratuitos, la mayoría de ellos en inglés. Los usuarios pueden acceder a los libros pero no pueden copiar o distribuir el material con propósitos comerciales sin el debido permiso. Por ejemplo, en "Archive.org" es posible encontrar "El mago de Oz", mientras el Centro de Texto Electrónico de la Universidad de Virginia tiene una biblioteca que cuenta con 1800 títulos, incluidos clásicos como "Alicia en el País de las Maravillas", de Lewis Carroll; "El origen de las especies", de Charles Darwin; "Moby Dick", de Herman Melville; y "Cumbres Borrascosas", de Emily Bronte. Mientras, el "Project Gutenberg", permite a la gente descargar copias de clásicos, la mayoría libros escritos antes de 1923, cuyos derechos de autor han expirado, como las obras de Shakespeare, Conan Doyle y la Biblia.

Un caso reciente: Google y Amazon están poniendo a disposición al público obras literales completas. Esto ha generado una gran discusión, un gran reclamo, amenazas y demandas judiciales concretas por parte de la industria editorial, porque aún cuando la obra sea de dominio público las editoriales se ven afectadas.

Las historias e iniciativas que les he narrado, y muchas otras más, demuestran la importancia de que todos los que estén involucrados en la industria y difusión del libro, y en general, de la protección documental, no sólo conozcan las posibilidades que nos da la tecnología para acceder a esa información, sino también los conceptos básicos de la protección jurídica de la propiedad intelectual, así como la normativa penal que establece y sanciona como delictivas ciertas conductas violatorias de estos derechos.

No hay que olvidar que vivimos también una época no solo de colaboración e interacción intelectual, sino que mucho de nuestro tiempo libre ahora se aprovecha en la Web. El trabajo de actualización y

de alimentación de una fuente global de información como es Wikipedia, por ejemplo, sería imposible sin las más de 100 millones de horas usuario[2] que proveen los internautas de manera gratuita a dicha tarea. El proyecto de una enciclopedia global sobre todos los temas imaginables se está traduciendo en el proyecto de colaboración pública más intensiva de la historia de la Humanidad. Sin duda, una muestra de las cosas que se pueden lograr positivas en las actuales condiciones de desarrollo del ambiente de la información en la "Red de Redes".

La protección jurídica de la propiedad intelectual en Internet

Una manera sencilla de definir la Propiedad Intelectual es indicar que esta hace referencia a un derecho exclusivo sobre las invenciones y expresiones creativas, ya que estas tienen un importante valor personal, cultural e incluso comercial. Así, dentro de este concepto de propiedad intelectual podemos incluir tanto lo referente a la propiedad literaria o artística (es decir, a los derechos de autor y derechos conexos) a la propiedad industrial (que hace referencia a patentes, diseños industriales y marcas, entre otros), a los derechos derivados de las obtenciones vegetales y de los esquemas de trazado de los circuitos integrados, y a los secretos comerciales e industriales (la llamada "información no divulgada").

Los derechos de autor protegen la integridad de las creaciones de artistas y autores, así como el interés de la sociedad en promover esas creaciones. Los derechos conexos son aquellos que protegen los

2 *Dato proveído por la Revista Wire de los Estados Unidos en un artículo de 2010 sobre los cambios en la actividad de las personas que han empezado a utilizar de manera distinta su tiempo libre. Los autores del reporte comparan las más de 100 billones de horas de televisión que suelen utilizar los usuarios en los Estados Unidos con las otras que son necesarias para actualizar los contenidos de la Wikipedia, y ven en ello un cambio de radical importancia en las prácticas sociales, la predisposición a la solidaridad y a utilizar de manera inteligente el tiempo libre. Se trata de una tendencia creciente fomentada, también, por las redes sociales y las nuevas formas de interacción social provocadas por nuevos servicios en Internet.*

intereses de artistas intérpretes o ejecutantes, productores de grabaciones y organismos de radiodifusión en relación con sus actividades referentes a la utilización y difusión pública de obras de autores.

El hecho que un contenido haya sido "subido" a Internet, con el fin de compartirlo y promover su conocimiento, no significa que cede los derechos de autor. La usual expresión *"estaba en Internet y de lo ahí lo cogí"* no significa que se trate de un ámbito libre de regulación, donde pueden promoverse daños a los derechos protegidos en la legislación bajo análisis.

Las normas fundamentales de protección a la propiedad intelectual no sólo son de rango legal, también la Constitución Política costarricense así como disposiciones de derechos humanos contenidas en declaraciones y convenciones en la materia, promueven la tutela de los derechos autorales. Es así como se orientan los textos del artículo 47 de nuestra Carta Magna, el artículo XIII de la Declaración Americana de los Derechos y Deberes del Hombre de 1948, el artículo 27 de la Declaración Universal de Derechos de Humanos (adoptada y proclamada por la Asamblea General de la Organización de Naciones Unidas en su resolución 217 (III), de 10 de diciembre de 1948). En igual sentido se orientan los Convenios de Berna y Roma y el mismo Tratado de la OMPI -Organización Mundial de la Propiedad Intelectual- sobre derechos de autor), y a nivel nacional. A nivel legal, por supuesto, contemplan protección para los derechos autorales, la Ley de Derechos de autor, que ha sido recientemente reformada, y la Ley de Procedimientos de Observancia de los derechos de propiedad intelectual, que es la que enumera los delitos.

Es importante señalar que lo que el derecho de autor protege no son las ideas en sí mismas consideradas, sino su forma de expresión, el modo en que las ideas se manifiestan. Por ejemplo, la idea de que el mar es un lugar muy hermoso no está protegida y nos pertenece a todos. Lo que sí esta protegido es, por ejemplo, la forma en que el poeta Rubén Darío lo dice: *"Margarita, está linda la mar, y el viento lleva esencia sutil de azahar..."*[3]

3 "A Margarita Debaile" de Rubén Darío.

Además, la protección de los derechos de autor se da en dos ámbitos: por un lado, la protección de la paternidad intelectual e integridad de la obra; y por otro, la protección de la exclusividad temporal de explotación comercial –económica- de ese derecho. En el primer caso, estamos hablando de los llamados "derechos morales de autor" (que básicamente se centran en el reconocimiento de la persona del autor, y la posibilidad que este tiene para oponerse a que otro se haga pasar por el autor de su obra, el derecho de exigir que la obra siempre indique su nombre en calidad de autor, y el derecho a oponerse a su mutilación o alteración, así como el de autorizar su uso). Estos derechos son perpetuos y personales[4].

Por su parte, los derechos patrimoniales consisten en las ganancias derivadas de la producción de la obra y su comercialización. Estos son transmisibles (por ejemplo, es lo que se hace, en concreto, mediante un contrato de cesión de derechos de autor a una editorial), y además son temporales, ya que las normas establecen que esta protección del ámbito patrimonial finaliza 70 años después de la muerte del autor. Luego, las obras pasan a ser de dominio público, patrimonio de uso común de la humanidad.

La protección jurídica de los derechos de autor se da en varias ramas del derecho. Por ejemplo, civilmente es posible exigir indemnizaciones por daños y perjuicios ocasionados por actividades lesivas de estos derechos, tanto de los patrimoniales como de los morales. Sin embargo, me centraré en la normativa penal.

En nuestra Ley de Procedimientos de Observancia el legislador creó delitos para cada categoría de derechos. Con esto quiero decir que los tipos penales precisaron los objetos de su protección y no usaron una fórmula general (como "propiedad industrial" o "propiedad artística" o "derechos de autor"). Cada norma penal establece con claridad cuál es el bien jurídico que protege: las obras literarias, las obras artísticas, los fonogramas, las emisiones -incluidas las satelitales-, etc.

4 Cfr. Artículo 14 de la Ley de Derechos de Autor.

Cabe indicar que los delitos contra derechos de patentes de invención, dibujos y modelos industriales y modelos de utilidad y los delitos contra la información no divulgada que se habían creado en el año 2000, fueron derogados en las reformas legislativas del año 2008. Subsisten los delitos en materia de derechos de autor y derechos conexos, marcas y signos distintivos y los referentes a los trazados de circuitos integrados.

Los tratados internacionales como el ADPIC y los tratados de la Organización Mundial de Propiedad Intelectual, OMPI, en materia de derechos de autor y derechos conexos, han establecido que la protección de estos derechos se extiende a las nuevas tecnologías y al entorno digital.

Los derechos de autor y derechos conexos en el ámbito multimedial

Los derechos de autor protegen, entre otros aspectos:

- Las obras artísticas, científicas, literarias, en un sentido muy amplio.
- Las bases de datos especializadas, siempre y cuando la disposición de sus elementos sea suficientemente original, independientemente de la protección que tengan los datos contenidos en ellas; obviamente, la persona que los recolectó y compiló tiene los derechos de compilación.
- También los programas de cómputo. Sobre estos, actualmente se reconoce la posibilidad de tener una copia para uso personal y también de hacer algunas modificaciones para determinados usos. En el reglamento se establece esto más detalladamente.

Uno de los principios fundamentales que viene de los tratados internacionales es el de Informalidad, que significa que el surgimiento de los derechos de una persona sobre su obra artística –en un sentido bien amplio, incluyendo la obra literaria, las páginas Web y las obras audiovisuales- surge simplemente por el hecho de la creación de la obra, por su materialización, siempre que esta sea original, por lo que no se requiere ninguna formalidad registral para que vengan a la obra inmediatamente los derechos de propiedad intelectual.

Así lo establecen los convenios y los tratados internacionales, incluso nuestra ley, pues las obras se registran sólo por seguridad.

Es muy difícil regular estas materias, precisamente porque el ámbito de Internet es casi un ámbito jurídico irregular, rebelde a la regulación y al control, y organizado, por la propia lógica del sistema, de una manera no jerárquica. Esto provoca, por una parte, la multiplicidad de regulaciones nacionales enfrentadas a las reglas internacionales, los problemas de jurisdicción y, por otra parte, el carácter multinacional de las infracciones.

El derecho a la información, en efecto, es muy importante para el desarrollo de los países, y el libre acceso a datos, informaciones y contenidos de relevancia científica, técnica y artística garantiza, por supuesto, el mejoramiento de las condiciones generales de vida de las personas. Internet colabora en esta función, todos los días. Sin embargo, es necesario que los internautas incorporen protocolos de conducta en sus actividades de uso de la red para evitar la infracción a derechos autorales.

Los motores de búsqueda facilitan el acceso a los contenidos. La aparición de referencias a textos, libros y links con información de los lugares donde se encuentran obras protegidas no es, de suyo, un delito, ya que sólo dan referencia al sitio donde pueden ser encontrados y tienen, en esencia, la utilidad que podría tener, en el contexto de una obra escrita, por ejemplo, la cita al pie de página, que da constancia de la fuente bibliográfica consultada. Además, el autor que ha subido su obra a Internet, de cualquier forma, asume la posibilidad de que los motores de búsqueda ubiquen el link de su obra para facilitar su acceso y consulta. No se trata de un peligro sino de un "riesgo permitido" y que se explica y justifica, en general, por el uso de Internet para fines científicos, literarios o artísticos.

Cuando se trata de servidores que ponen textos y obras libres para el acceso a los internautas, resulta exigible que estos recaben el consentimiento expreso de los autores. Si el autor ha subido su información a un *blog* libre o a una página de almacenamiento gratuito suponemos que ha dado su consentimiento tácito a que estas informaciones estén

al servicio de las personas que lo consultarán en Internet. Si se trata de páginas de consulta de información previo pago, este consentimiento tiene que ser expreso ya que quienes cobran por estos servicios están usufructuando derechos autorales de los dueños de la obra y por ello deben reconocer esos derechos patrimoniales por el uso del trabajo científico de alguien más.

A la par de los derechos de autor tenemos los derechos conexos, que son los derechos que corresponden a artistas intérpretes, artistas ejecutantes, productores de fonogramas y también a los organismos de radiodifusión, sean personas físicas o jurídicas.

Estos derechos de autor, como puede imaginarse, viven tiempos difíciles en la Web. Junto a los escenarios vistos, tenemos también el problema de las conexiones P2P *"peer to peer"*. Hay conexiones de este tipo puras o híbridas, en cualquiera de sus modos de existencia, tenemos que en cada nodo las computadores conectadas operan al mismo tiempo como "clientes" y como "servidores", de tal manera que los contenidos compartidos por unos pueden ser utilizados por otros que se conecten de la misma manera. Los servicios P2P "recuerdan" cuál computador tiene cuál información y las ponen al servicio de todos los que la busquen, facilitando la información mediante interconexión de los contenidos en línea. *"Napster"*, que nació en el año 1999, fue la primera experiencia en este sentido, pero fue cerrada en el año 2001 por una demanda presentada ante ese servicio de intercambio de música. Ante su desaparición surgieron servicios similares como "Kazaa", "Edonkey", "Morpheus", "Grokster", "Emule" y "Torrent". Estos servicios principalmente comparten contenidos musicales, pero abrieron la puerta para el uso de otros tipos de informaciones que también son buscados por los internautas.

Las redes *peer to peer* han provocado actividad judicial de la industria discográfica para tratar de impedir, en primer lugar, el intercambio de los contenidos pero también generar cánones que pudieran indemnizar los daños económicos ocasionados por el funcionamiento de estos servicios.

Algunos temas penales relevantes

En el año 2000 las penas de los delitos eran de uno a tres años de prisión. En el año 2008 se reformó y adicionó la Ley de Procedimientos de Observancia de los Derechos de Propiedad Intelectual, especialmente en la materia de los delitos y se efectuaron cambios sustanciales: se reformularon los tipos penales existentes, se introdujeron nuevas figuras penales, se incluyó en algunos delitos figuras de excusas legales absolutorias, se ampliaron los plazos de las penas de prisión y se incorporaron nuevos tipos de sanciones, ya que, además de las penas de prisión, se incluyeron como penas alternativas las penas pecuniarias; y tanto los años de las penas de prisión, como las multas en las penas pecuniarias se presentan en forma gradual ascendente según ascienda el monto del perjuicio. En algunos casos se estableció pena de prisión hasta de un máximo de cinco años.

El problema de la magnitud de las penas o sanciones implica un conflicto entre aquellos que impulsan su aumento y aquellos que favorecen más bien su disminución. Pero la Sala Constitucional dijo que el establecimiento de penas en esos márgenes es una manifestación de política criminal que no lesiona el principio de proporcionalidad.

También es interesante analizar otros puntos contenidos en esta legislación. Uno de ellos se refiere al llamado "principio de lesividad". La norma del año 2000 contenía un artículo donde expresamente se establecía este principio.

El principio de lesividad, incluido en forma expresa en la ley constituía un "focus" de atención ya que considera que no toda acción puede ser considerada como delito, sino aquella que lesiona en cierto grado los valores o derechos protegidos, de modo que las actividades que sólo infringen lesiones muy leves o insignificantes no son sancionadas.

Penalmente, en términos generales, se reconoce este principio a nivel procesal. Sin embargo, algunos sectores manifestaban su descontento con su inclusión en la Ley de Procedimientos de Observancia y en diversos proyectos de ley habían propuesto su derogación.

Hay que reconocer que la inclusión de este principio en una normativa especial podría inducir a los operadores jurídicos, si no cuentan

con un conocimiento adecuado de la materia de propiedad intelectual, de los principios que la regulan y de las normas procesales penales generales, a abusar de esta consideración en perjuicio de una protección eficaz a los derechos y valores tutelados por estas leyes, pues podrían minusvalorar las lesiones provocadas por los actos delictivos de particulares, optando por aplicar indiscriminadamente el criterio de insignificancia.

Otro tema que fue objeto de discusión entre los distintos grupos de interés relacionado con los delitos contra la propiedad intelectual es el de la naturaleza de la acción penal. La acción penal es el derecho que tiene el Estado de perseguir y juzgar a un delincuente. Frente a ella, los delitos se clasifican en tres tipos: de acción pública, de acción pública perseguible a instancia privada, y de acción privada. En el primer caso, la persecución la inicia el Estado de oficio, por medio de sus órganos judiciales, sin que sea necesario la denuncia del titular del derecho. En el segundo caso, el Estado actúa únicamente si el damnificado solicita su intervención. La ley de procedimientos de observancia de los derechos de propiedad intelectual estableció que los delitos eran de acción pública a instancia privada. Con ello, únicamente podrán juzgarse aquellas conductas que sean denunciadas por los autores o los titulares legítimos de los derechos de autor o un derecho de propiedad intelectual. El tema es controversial, ya que mientras algunos sectores han sostenido la necesidad de que se reforme la ley con el fin de que la acción penal sea de "acción pública", otros sectores sostienen que permanezca como "acción pública a instancia privada".

El legislador probablemente tomó en cuenta que obligar al Ministerio Público a una persecución de estos hechos por acción pública implica un compromiso que debe integrarse con la política general que se haya construido a lo interno de ese órgano con otra gran cantidad de delitos contemplados en las demás leyes penales. Lo anterior califica un problema práctico ineludible, ya que los esfuerzos de investigación y represión serán directamente proporcionales a los medios y recursos del órgano judicial para poder orientar su política de persecución, la cual debe administrarse con otra gran cantidad de conductas delictivas también de interés para la colectividad.

Además, de las razones prácticas apuntadas, existe una razón de derecho sustantivo que consiste precisamente en el interés de persecución por parte de la víctima. El tipo de bienes jurídicos que están implícitos en los derechos de autor y conexos necesitan que haya una afectación personal a los titulares de esos derechos, es decir, que la relación de disponibilidad específica que subyace al objeto de protección sea efectivamente lesionada, esto es, que tiene necesariamente que haberse demostrado una afectación o posibilidad de afectación con el actuar de una persona determinada. Esto es de difícil constatación por parte del Ministerio Público, sobre todo cuando se trata de ejercicios de derechos y hasta de expectativas jurídicas derivadas de normas positivas que contemplan la realización práctica de ciertos derechos implícitos.

Obsérvese por ejemplo la dificultad de saber cuándo una obra intelectual ha sido lesionada por alguien si dicha obra tiene difícil acceso por el público o es poco conocida. O por el contrario al estar la obra a disposición del público, no podría el Estado de oficio suponer el dolo, ni conocer si hubo o no autorización del titular de la obra para esa puesta a disposición, o para que esta fuera reproducida. En estos casos sólo la acción directa del afectado, poniendo la notitia criminis es la que puede incoar los procesos penales correspondientes que puedan tener por objetivo la investigación y sanción de los hechos antijurídicos.

En los casos de leyes de propiedad intelectual es importante que se haga constar siempre el interés personal en la persecución; y al efecto las leyes procedimentales contemplan una serie de posibilidades que les permiten a las víctimas de un delito ejercer directamente sus derechos incluso cuando el Ministerio Público no considera oportuna la persecución. Entre estos mecanismos procesales tenemos el querellante particular y el querellante adhesivo.

En síntesis, parece que lo considerado por el legislador como más conveniente fue que la incoación del proceso penal fuese por instancia privada pero dentro de un marco de acción pública. Consultado el Ministerio Público y otras instancias judiciales sobre este tema consideraron que esto último no sólo produce mejores efectos para la averiguación de hechos en contra de derechos de autor y conexos, sino también una adecuada formación de la causa con los datos que los afectados puedan aportar para el trabajo de ese Ministerio.

La doctrina jurídica señala que estos delitos son no convencionales, no tradicionales, delitos económicos y de difícil persecución. Sobre esto, comparto una idea que esboza el penalista español José Manuel Paredes Castañon, a propósito de la materia de patentes, que se podría aplicar a los delitos contra los derechos de autor:

"si existen numerosos problemas teóricos en la delimitación de los tipos, más numerosas aún son las dificultades prácticas a la que se enfrenta el aplicador del Derecho Penal a la hora de hacer valer la eficacia de éste en la protección de los bienes jurídicos y en la prevención de conductas peligrosas para los mismos, cuando éstas se generan –como es el caso- en el ámbito de la empresa. Al respecto, hay que tener en cuenta que existe un problema de partida (...), que es el relativo a la selección de los intereses que han de merecer protección penal en el ámbito del tráfico patrimonial. Pues lo cierto es que, más allá de los delitos patrimoniales tradicionalmente configurados, la realidad económica y empresarial enfrenta al Ordenamiento Jurídico a nuevos –o nuevamente intensificados- fenómenos de conductas antisociales, frente a las que parece ineludible la reacción represiva; pero ante las que muchas veces no existe un toma de posición político criminal suficientemente clara que permita determinar con fundamento bastante cómo ha de ser dicha reacción (tanto la tipificación como la sanción)".

En cuanto a las características de estos delitos, en la mayoría de los tipos penales en derechos de autor presentan, entre otras, las siguientes :

- El medio para cometer el delito es cualquier medio o herramienta.
- Su modo es "de manera que cause perjuicio".
- Se pueden cometer en cualquier momento y lugar.
- Poseen un sujeto activo indeterminado: cualquiera puede cometerlos.
- El sujeto pasivo también puede ser cualquiera, siempre que sea el titular de los derechos afectados.
- Se trata de delitos dolosos.

La Sala Constitucional, en distintas resoluciones –sobre todo en la 4530-2000–, ha señalado que ninguna acción humana pueda constituir delito, sino la define como tal una ley anterior que dicte el órgano competente. Esto es lo que se conoce como principio de tipicidad. Además, los tipos penales deben estar estructurados como una proposición condicional, que consta de un presupuesto (descripción de la conducta) y una consecuencia (pena); en la primera debe necesariamente indicarse, al menos, quien es el sujeto activo y cuál es la acción constitutiva de la infracción; sin estos dos elementos básicos puede asegurarse que no existe tipo penal.

Por lo tanto, existe una obligación legislativa, (a efecto de que la tipicidad sea una verdadera garantía ciudadana), de utilizar técnicas legislativas que permitan tipificar correctamente las conductas que se pretenden reprimir como delito, y ello se encuentra enteramente relacionado con el mayor o menor grado de concreción y claridad que logre el legislador.

La necesaria utilización del idioma y sus restricciones obliga a que en algunos casos no pueda lograrse el mismo nivel de precisión. El establecer el límite de generalización o concreción que exige el principio de legalidad debe hacerse en cada caso particular.

Además de la tipicidad, el Principio de Proporcionalidad en esta misma materia obliga a ponderar la gravedad de la conducta, el objeto de tutela, y la consecuencia jurídica.

Hechos delictivos generados por la consulta de obras en Internet

Cuando se realizan investigaciones científicas o se preparan trabajos es usual la consulta de fuentes disponibles en Internet. Gracias a ello se cuenta con información actualizada, y dependiendo de la fuente, también fiable sobre diversas temáticas de interés. Sin embargo, el hecho de que la información esté en Internet y no se disponga de su autor, no es una certeza de que la información pueda ser reproducida sin permiso.

Veamos:

- Por ejemplo, se tiene como autor de la obra protegida, salvo prueba en contrario, al individuo cuyo nombre o seudónimo conocido esté indicado en ella, en la forma habitual.
- Una gran cantidad de obras que se encuentran a disposición del público no contienen información sobre su autor o autores u otra información definida en la ley como "información para la gestión de los derechos". Dado el principio de informalidad, el gran público debe presumir la existencia de derechos de propiedad intelectual sobre la obra, aún es tando a su disposición de forma tal que sea éste (el público) quien decida cuando y desde dónde accede a ella; y de tratarse de una obra protegida éste (el público) desconoce, su plazo de protección. Recordemos que el autor o titular de la obra tiene el derecho exclusivo de autorizar o no la puesta a disposición del público de su obra de forma tal que este sea el que decida cuando y desde donde accede a ella. Este es un derecho patrimonial, independiente de otros derechos, como el de reproducción y traducción. Es decir, aún si el titular del derecho autorizara la disposición al público de la obra, no necesariamente, implica la autorización para reproducir o traducir; cada derecho es independiente.
- La Ley establece una serie de excepciones o limitaciones a los derechos exclusivos. Así el artículo 67 de la ley de derechos de autor establece que las noticias con carácter de prensa informativa no gozan de la protección de esta ley; pero que el medio que las reproduce o retransmite está obligado a consignar la fuente original de dónde se tomó la información.
- También los artículos de actualidad, publicados en revistas o periódicos, pueden ser reproducidos, si ello no ha sido expresamente prohibido, debiendo -en todo caso- citarse la fuente de origen. (artículo 68).
- Otras obras que pueden publicarse tanto en prensa o radio o TV sin necesidad de autorización son los discursos pronunciados en las asambleas deliberadas o en reuniones públicas y los alegatos ante los tribunales de justicia; pero estos no pueden

publicarse en impreso separado o en colección sin el permiso del autor (artículo 69).

- Todos, cuando hacemos una investigación, citamos textualmente ideas de otras personas, que nos sirven como argumento a favor de las nuestras, o simplemente como ilustración. ¿Son las citas textuales algo permitido por la ley? Por supuesto. Sin embargo, la ley aclara que es permitido citar a un autor, transcribiendo los pasajes pertinentes, siempre que éstos no sean tantos y seguidos, que puedan considerarse como una reproducción simulada y sustancial, que redunde en perjuicio del autor de la obra original (artículo 70).

Hechos delictivos generados por la reproducción de material protegido por derechos de autor vía Internet y otros medios de comunicación multimedial.

Podemos imaginar otros contextos problemáticos, sobre todo aquellos relacionados con la transmisión no autorizada de contenidos en blogs, páginas web o redes sociales, de contenidos protegidos por derechos de autor, las siguientes reflexiones pretenden indicar algunas temáticas que podrían estar involucradas en esos escenarios de eventual antijuridicidad:

- En tesis de principio, se pueden reproducir fotográficamente o por otros procesos pictóricos las estatuas, monumentos y otras obras de arte adquiridos por el poder público, que estén expuestos en calles, jardines y museos (artículo 71).
- También está permitida la ejecución de discos y recepción de transmisiones de radio o TV en los establecimientos comerciales que venden aparatos electrodomésticos o fonogramas para demostración a su clientela (artículo 72).
- Son libres las interpretaciones o ejecuciones de obras teatrales o musicales, que hayan sido puestas a disposición del público en forma legítima, cuando se realicen en el hogar para beneficio exclusivo del círculo familiar. También serán libres dichas interpretaciones o ejecuciones cuando sean utilizadas a título de ilustración para actividades exclusivamente educativas, en la medida justificada por el fin educativo, siempre que dicha interpretación

o ejecución no atente contra la explotación normal de la obra ni cause un perjuicio injustificado a los intereses legítimos del titular de los derechos. Adicionalmente, deberá mencionarse la fuente y el nombre del autor, si este nombre figura en la fuente.

- Asimismo, es lícita la utilización y reproducción, en la medida justificada por el fin perseguido, de las obras a título de ilustración de la enseñanza por medio de publicaciones, tales como antologías, emisiones de radio o grabaciones sonoras o visuales, con tal de que esa utilización sea conforme a los usos honrados y se mencionen la fuente y el nombre del autor, si este nombre figura en la fuente.
- El derecho de copia privada está también incluido en la ley, que indica que es libre la reproducción de una obra didáctica o científica, efectuada personal y exclusivamente por el interesado para su propio uso y sin ánimo de lucro, pero la misma ley establece que esa reproducción deberá realizarse en un solo ejemplar, mecanografiado o manuscrito, y que esta disposición no se aplica a los programas de cómputo (artículo 74).
- Todos podemos reproducir libremente las constituciones, leyes, decretos y otras normas generales, pero tenemos la obligación de ajustarnos estrictamente con la edición oficial. Podemos publicar los códigos y colecciones legislativas, con notas y comentarios, y cada autor será dueño de su propio trabajo. También es libre la publicación del retrato cuando se relaciona con fines científicos, didácticos o culturales, o con hechos o acontecimientos de interés público, o que se hubieran desarrollado en público (artículos 75 y 76).
- En relación con los derechos exclusivos de los artistas intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusión, son permitidas las siguientes excepciones, siempre y cuando no atenten contra la explotación normal de la interpretación o ejecución, del fonograma o emisión, ni causen un perjuicio injustificado a los intereses legítimos del titular del derecho:

a) Cuando se trate de una utilización para uso privado.

b) Cuando se hayan utilizado breves fragmentos con motivo de informaciones sobre sucesos de actualidad.

c) Cuando se trate de una fijación efímera realizada por un organismo de radiodifusión por sus propios medios y para sus propias emisiones.

d) Cuando se trate de una utilización con fines exclusivamente docentes o de investigación científica.

Sin perjuicio de lo dispuesto en el párrafo 1 de este artículo y en el artículo 83 de esta Ley, no es permitida la retransmisión de señales de televisión (ya sea terrestre, por cable o por satélite) en Internet sin la autorización del titular o los titulares del derecho sobre el contenido de la señal y de la señal.

Conclusiones:

La Propiedad Intelectual está ligada al desarrollo científico, socioeconómico y cultural del país, pues abarca, entre otras categorías, los derechos de autor, las patentes de invención, los conocimientos tradicionales, los secretos comerciales e industriales, y la competencia.

La Propiedad Intelectual está protegida por la Constitución Política de Costa Rica y una sólida normativa sobre las distintas categorías propias de la materia. Existen además, organizaciones y tratados internacionales de los que Costa Rica forma parte, los cuales establecen obligaciones para la protección de los derechos de Propiedad Intelectual. La protección penal alcanza sólo a los derechos de autor y derechos conexos y a las marcas y signos distintivos.

Es importante discutir y reconocer cuáles son los compromisos de carácter internacional en la materia de propiedad intelectual y analizar la pertinencia, necesidad, concreción, coherencia y congruencia del desarrollo de la normativa nacional objeto de aprobación legislativa reciente.

De momento la equiparación normativa alcanzada con ADPIC y CAFTA-DR tendrán incidencia en la región, pero esto no se puede decir de todos los países del mundo.

En la práctica, si se quiere cumplir las normas y perseguir efectivamente los delitos, se necesita muchos más medios, más infraestructura.

Los compromisos vigentes en la normativa internacional delimitan el uso del derecho penal como un medio para castigar la piratería lesiva de derechos de autor y derechos conexos, la discusión entonces, deberá centrarse en cómo lograr que las normas penales cumplan el objetivo y que a la vez se ajusten a los principios vigentes de nuestro estado de derecho como la proporcionalidad, razonabilidad, tipicidad penal, principio de inocencia, debido proceso, y su equilibrio con la protección de otros derechos fundamentales como el acceso a la educación, la cultura y la información.

Considerando que el ciberespacio es un ámbito donde se cometen la mayoría de los delitos del mundo físico y que la diferencia está en las dificultades de persecución se debe analizar si estas formas tradicionales de tipicidad penal son aplicables al entorno digital, o este requiere de normas específicas o más desarrolladas que enfrenten las dificultades de persecución penal de conductas cometidas en el ciberespacio.

Fuentes:

Constitución Política de la República de Costa Rica (artículos 47, 89,121 inciso 18).

Declaración Universal de Derechos Humanos (artículo 27).

Declaración Americana de los Derechos y Deberes del Hombre.

Convenio que establece la Organización Mundial de la Propiedad Intelectual, OMPI, firmado en Estocolmo el 14 de julio de 1967, aprobado mediante Ley No. 6468 de 18 de setiembre de 1980.

Ley 7475 Anexo 1-C de la Convención que crea la O.M.C. “Aspectos de los Derechos de Propiedad Intelectual y el Comercio” (ADPIC) o conocido por sus siglas en inglés (TRIP’s).

Convenio de Berna para la protección de las obras literarias y artísticas, Ley #6083 del 27 de setiembre de 1977.

Convención Internacional sobre la protección de los artistas intérpretes o ejecutantes, los productores de fonogramas y los organis-

mos de radiodifusión (“Convención de Roma, 1961”), Ley # 4727 del 13 de marzo de 1971.

Convención Universal sobre los Derechos de Autor (“Convención de Ginebra”) y sus dos protocolos (París, 1971), Ley #5682 del 4 de junio de 1975.

Convención para la protección de los productores de fonogramas contra la reproducción no autorizada de sus fonogramas, Ley No.6486 del 5 de noviembre de 1980.

Convenio de Bruselas sobre la distribución de señales portadoras de programas transmitidas por satélite (1974), Ley No. 7829 del 16 de octubre de 1998.

Ley 7967: Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas (WPPT) (1996). Publicado en la Gaceta No. 21 del 31 de enero del 2000.

Ley 7968: Tratado de la OMPI sobre Derechos de Autor (WCT) (1996). Publicado en la Gaceta No. 23 del 2 de febrero del 2000.

Ley Nº 8622, Publicada el 21 de Diciembre de 2007, Gaceta Nº 24 Tratado De Libre Comercio entre Republica Dominicana, Centroamerica y Estados Unidos Relacionadas con la Propiedad Intelectual .

Ley de Procedimientos de Observancia de los Derechos de Propiedad Intelectual, Ley No. 8039 y sus reformas.

Ley de derechos de autor y derechos conexos, Ley #6683 del 4 de noviembre de 1982 y sus reformas.

Ley No. 8656 del 18 de julio de 2008Reforma y adición de varios artículos de la Ley de Procedimientos de Observancia de los Derechos de Propiedad Intelectual, Ley Nº 8039 del 12 de diciembre de 2000.

Sitio Web: Organización Mundial de la Propiedad Intelectual. www.ompi.int.

Capítulo 6
Las TIC y la Seguridad Nacional

Tecnologías de la información y prevención del riesgo

Mauricio Mora Fernández

El desarrollo de la sociedad conlleva el uso de recursos naturales y con ello las múltiples maneras de utilizar la superficie del planeta y los recursos que hay sobre y debajo de su superficie. No obstante, el aumento del riesgo es la consecuencia clara del camino equivocado que ha tomado el ser humano para alcanzar dicho desarrollo. En otras palabras, los desastres han puesto reiteradamente en evidencia todos los problemas de índole: cultural, político, social, económico y administrativo, que se acumulan en el tiempo y que incrementan la vulnerabilidad en una región determinada. Por lo tanto, en el marco de la gestión del riesgo, el desastre es concebido como una construcción social, producto de las modificaciones e impactos negativos que produce el ser humano en su entorno, como consecuencia de sus actividades.

En Costa Rica, como en otras partes del mundo, el camino que conduce a la construcción del riesgo tiene comunes denominadores, entre los más importantes están, en primer lugar, la falta de un ordenamiento territorial adecuado lo cual hace que se ubiquen asentamientos humanos en áreas donde existen uno o varios procesos naturales que, de manera individual o concatenada, pueden

convertirse en amenazas. De la misma manera, también ocurre que se desarrollan asentamientos humanos cerca de zonas industriales cuya actividad puede convertirse con el tiempo en una amenaza. Posteriormente podemos enunciar otros denominadores como: la falta de políticas de gestión de los recursos naturales, particularmente el agua; la falta de una gestión ambiental adecuada de los múltiples desechos generados por la actividad humana; el deterioro de la calidad de vida de la sociedad y empobrecimiento; la falta de una gestión administrativa adecuada por parte del gobierno en lo referente a prevención y atención de emergencias así como los intereses políticos, económicos y privados.

En Costa Rica hay ejemplos muy claros donde convergen los factores anteriores que, en conjunto con los procesos naturales, hacen muchas regiones propensas a los desastres. Para citar un caso, los valles de los ríos Buenavista, Chirripó Pacífico y del General constituyen una región donde ocurren múltiples procesos geológicos disparados tanto por procesos internos (sismos) como hidrometeorológicos (inundaciones y deslizamientos). La expansión de los asentamientos humanos en esa región ocurre principalmente en los valles aluviales pero, cada día, hay más presión sobre las zonas de topografía más abrupta.

Por otra parte, desde el punto de vista social, las migraciones han dado un claro matiz de género, al ser la mujer en gran medida, la que debe afrontar el sostenimiento del hogar y, en consecuencia, la que enfrenta el proceso de desastre. Además el ingreso de la población extranjera, principalmente de origen estadounidense, ha generado un mercado de la tierra no planificado, en donde muchos campesinos, al querer evadir los problemas que enfrenta el sector primario, vende sus tierras para convertirse de propietario a proletario y peón en sus antiguas tierra, o bien, migren a la ciudad en donde normalmente no tienen los medios adecuados para subsistir. Además esto ha genera impactos en las costumbres autóctonas que en muchos casos es negativo y conlleva el deterioro social por pérdida de la memoria colectiva y por el desarraigo.

En la actualidad, con el desarrollo de la tecnología, es común la utilización de herramientas, como los Sistemas de Información Geográficos o complejas estructuras de bases de datos, para estudiar no solamente los procesos naturales por si solos, sino también combinados con la complejidad de los procesos sociales para comprender el impacto de una amenaza determinada y con ello tomar las medidas correctivas o preventivas necesarias. Sin embargo, es importante tener claro que, en cualquier análisis de amenaza, de vulnerabilidad o de riesgo, es fundamental considerar los siguientes aspectos:

- La calidad de la información con la cual se alimentará la tecnología.
- Las ventajas y limitaciones de la tecnología que se utiliza y si se adapta o no al objeto y área de estudio.
- Los procesos naturales pueden actuar solos o concatenados, particularmente en zonas multiamenazas donde convergen diferentes procesos naturales.
- Los procesos naturales carecen de límites administrativos, por lo tanto, una tecnología aplicada sin una visión de cuenca o considerando la dimensión del proceso y su impacto carece de sentido.
- Que el fin primordial es el bienestar y seguridad del ser humano. Por lo tanto, el análisis va más allá de la interpretación fría de una matriz de salida o de un mapa, por ende, no solamente se debe ser sensible en el análisis y la interpretación de la información, sino también, considerar la participación de la población ya que es ella la que convive con el proceso y cada persona tiene su manera de percibirlo.

Finalmente, el territorio de Costa Rica es finito y en él ocurren numerosos procesos naturales. Por lo tanto, es imposible prohibir las construcciones o bien trasladar frecuentemente pueblos bajo amenaza, lo cual resulta costoso no sólo económicamente sino socialmente. No se trata tampoco de vivir por necesidad o por voluntad, en un espacio que muestra diferentes peligros, sino que es necesario entenderlos y considerar como pertinente la adaptación de la cultura y del "modus vivendi" de las comunidades ante esos peligros potenciales.

Hay que aceptar que se vive en un territorio geológicamente muy dinámico y por ende, el uso adecuado de las tecnologías en conjunto con la toma de decisiones correctas, permite mitigar el impacto de los procesos naturales. Hay que concebir un ordenamiento territorial participativo, no rígido ni restrictivo, que nos permita asentarnos, aceptando que hay procesos peligrosos con los que debemos convivir y ante los cuales debemos prepararnos.

Sistemas de Información en la Prevención de los Desastres Naturales

Sergio Sánchez Castillo

El objetivo general de esta ponencia es dar algún insumo sobre el que hacer de la Comisión Nacional de Emergencias (CNE) en el tema de la prevención de desastres en Costa Rica utilizando nuevas tecnologías, las cuales podrían ayudar a implementar la seguridad del Estado Costarricense.

Desde el punto de vista de amenazas naturales, cabe preguntarnos ¿Será Costa Rica un país peligroso o con amenazas naturales potenciales?

Para responder está interrogante, pensemos por un momento en la ubicación geográfica de Costa Rica, en la zona inter-tropical, área de paso de tormentas tropicales, huracanes en el cinturón de fuego del Pacífico, efectivamente, es una de las zonas con mayor sismicidad en el mundo al igual toda la costa pacífica de América, donde se gestan procesos de subducción muy fuertes desde las rocallosas en Norte América hasta los Andes en Sur América, de modo que la misma Centroamérica no se escapa de tal amenaza.

Amenazas geológicas

En el año 1997 el Geomar-UCR y la Universidad de Kiel, Alemania hicieron un mapeo de piso oceánico pacífico de la costa de Nicaragua y Costa Rica en donde se puede constatar el choque de placas Cocos y Caribe, generando la actual geomorfología de Costa Rica y Nicaragua, gracias a ese proceso de subducción tenemos una a diversidad de geo-formas, de microclimas, fallas locales, vulcanismo.

Este proceso de subducción de placa Cocos en la placa Caribe se estima en unos 88 mm – 92 mm en promedio anual, suficiente para denominarse como un territorio muy activo donde se generan levantamientos de nuestras cordilleras, actividad volcánica, fallas locales al interior de territorio nacional, por eso es necesario a la hora de planificar el paisaje ecológico tener en cuenta dichos factores para diseñar considerando períodos de retorno de fuertes sismos, urbanizar utilizando el código sísmico vigente, con diseños apropiados, tanto en edificios públicos (Hospitales) como en edificios privados, condominios, casas de habitación, puentes, carreteras.

Amenazas hidrometeorológicas

Por otra parte debemos recordar que América Central es una zona de paso depresiones tropicales, vaguadas, bajas presiones, frentes fríos y huracanes con un poder destructivo impresionante, como el caso del huracán Mitch, Floyd que han generado problemas muy graves en nuestras débiles economías.

Costa Rica por su ubicación geográfica, tiene una influencia oceánica severa, dado que es un territorio muy angosto de costa a costa, tal situación hace que cualquier sistema lo vuelve muy vulnerable y dispare una serie de incidentes al interior de nuestro país. Sumado a un sistema montano- volcánico en la parte central, áreas de inundación en el Caribe, las cuales se inundan en los meses de diciembre, enero y febrero por la entrada de los frentes fríos. En el litoral pacífico el período lluvioso se concentra de junio a noviembre se empiezan a presentar problemas de inundaciones en el pacífico Sur, Central, en especial en Parrita y finalmente en Guanacaste.

Durante la temporada de huracanes (junio-noviembre) estos sistemas se ubican en el océano Atlántico y en el mar Caribe provenientes de las costa de África, una vez frente a nuestras costas se mueven en contra de las manecillas del reloj en el hemisferio norte y succionan el viento del océano Pacífico generando abundante nubosidad y lluvias en nuestro litoral pacífico y de allí las consecuentes inundaciones en pacífico sur, central y Guanacaste, de esa misma manera se va atendiendo la emergencia y así se va moviendo toda la logística de las situaciones que van surgiendo.

Al interior del país, durante la época lluviosa suele presentarse problemas de inestabilidad de laderas, pequeños y grandes deslizamientos, flujos de lodo, como los que se han dado en Orosí, en el Alto Loaiza (2003, 2005) problemas en la red vial, como es el caso de la ruta 32 (San José-Guápiles), por eso es muy importante considerar la información geoespacial a la hora de planificar la construcción de infraestructura.

La ayuda de la tecnología

En este caso en Costa Rica se ha gestado varios proyectos sobre información espacial digital, a finales de los años 80 el proyecto *Sisvah* (Sistema de Información para el Sector Vivienda y Asentamientos Humanos), adscrito al Ministerio de Vivienda, con la cooperación de la Agencia Sueca. A mediados de la década de los 90 se gesto el proyecto Terra, con el cual se intento generar cartografía a escala 1:25.000. Ya para el presente siglo se llevaron a cabo las misiones Carta 2003 y Carta 2005, dentro del proyecto PRIAS, albergado en Centro de Alta Tecnología Dr. Franklin Chang Díaz, que involucran además de la tradicional fotografía aérea, la utilización de sensores multi-espectrales.

Posterior al terremoto de Cinchona el ICE, 2009 contrata una empresa privada para generar información geomorfológica actual a nivel de detalle (mm) utilizando un sensor llamado Lidar, el cual lanza una nube de rayos laser para reconstruir imágenes de increíble nitidez.

Hoy en día a través de los sistemas de información geográfica es posible hacer sobreposición de mapas con diferentes coberturas a saber: carreteras, ríos, puentes, áreas de inundación, fallas geológicas, deslizamientos, ciudades, centros poblado a diferentes escalas

y dependiendo de las geo-bases de datos espaciales se puede llegar a utilizar para ubicar personas, casas, hidrantes, teléfonos celulares. En Europa es normal y obligatorio estar inscrito en la estación de policía del barrio donde se habita, de esta manera hay un mayor control por parte del estado o del Ayundamiento sobre todo en temas de seguridad nacional. Lamentablemente en Costa Rica esto no se ha implementado, de hecho sería un tema a desarrollar por el Tribunal Supremo de Elecciones junto con otras instituciones, como Seguridad Pública, CCSS y la Municipalidad para hacer un sistema de información para ubicar a sus electores, habitantes, patronos, pacientes.

En Cañas, durante el año 2003 a través de proyecto Regional Action Programme Central America (RAP-CA) financiado por la UNESCO, se construyo una base de datos con la edad aproximada de las casas de habitación, el tipo de construcción, cuantas personas la habitan, si alguna persona que habita la casa tiene alguna incapacidad o enfermedad. Se consulto el cómo cocinan sus alimentos (leña, energía eléctrica, gas). Además, averiguo sobre los peligros cercanos a las viviendas, por ejemplo y si han tenido inundaciones, a cuantos centímetros o metros, luego él entrevistador en un croquis señala la cercanía de las viviendas a una estación de servicio, cercanía a paredón (amenaza de deslizamiento) o río, simultáneamente dicha información se ubica en un mapa de predios utilizando como base el catastro municipal.

Posteriormente se tabularon los datos y por fin se pudo sobreponer las diferentes coberturas interactuando con su respectiva base de datos geo-referenciada, para así determinar los primeros conflictos de uso de la tierra, eso se representa en un mapa y se logra determinar que ciertas personas, de ciertas casas podrían sufrir inundaciones porque estaban en el área, conocida como la llanura de inundación del río Cañas. O bien que las casas de madera en donde se cocinan los alimentos con leña y gas son más propensas a sufrir incendios.

La importancia de la información geo-espacial en la toma de decisiones

En Costa Rica hay varias ciudades que nacieron en valles inter-montanos, aéreas planas irrigadas por río y quebradas (Cartago, Santana, Turrialba, la misma Villa de la Boca del Monte). La ciudad de

Turrialba se ubica en la confluencia de varios ríos, además hay presencia de fallas geológicas y de alguna manera está expuesta a sufrir caída de cenizas del volcán que lleva su nombre, lo que la convierte en un área de multi-amenaza al igual que Cartago. Conociendo esta información es posible de alguna manera redefinir el uso actual de la tierra en la ciudad y proponer algunas soluciones que permitan mitigar y adaptar la ciudad con alguna planificación espacial mínima, evitando inversiones muy costosas en diques o obras que incluso podrían generar una falsa seguridad a sus habitantes, más bien sería más apto contemplar corredores (espacios a ambos lados de los ríos) para evitar que el río se estrangule y que pueda liberar su carga hidráulica en los espacios propuestos .

La construcción de escenarios espaciales, donde se involucran variables ambientales, sociales, económicas y hasta culturales, es lo que hemos tratado de ir elaborado en CNE esto nos ayuda mucho en la toma de decisiones. Los aportes de la Universidad de Costa Rica, específicamente de la Escuela Centroamericana de Geología, de la Escuela de Psicología, la información generada por los técnicos del ICE, de RECOPE de la escuela de Geografía de la Universidad Nacional ha sido fundamental en la construcción de los posibles escenarios ante un determinado evento.

Veamos un ejemplo, el escenario del volcán Arenal es uno de los más interesante no solo porque se logra construir un escenario de peligrosidad del volcán, sino porque el mismo esta respaldo por un decreto, que identifica restricciones en el uso de la tierra en los alrededores del volcán, es uno de los pocos que existe a nivel de América Central, fue realizado con la colaboración de muchos investigadores de la Universidad de Costa Rica, del OVSICORI y fue avalado por un experto vulcanólogo Teling, 2005.

Esto nos ayuda mucho a regular el uso de la tierra en los alrededores del volcán donde muchos inversionistas querían construir cabinas, pequeños hoteles, miradores, balnearios, áreas para acampar entre otros usos. Recordemos que el volcán Arenal es el más joven de Costa Rica y desde que empezó a eructar materiales no ha parado, es decir tiene 40 años eructando materiales, sin embargo también hay presiones para anular el decreto.

Vale mencionar que para algunos casos trabajamos escalas más detalladas para áreas, zonas especiales y problemáticas. En algunos casos se han elaborado modelos 3D, mapeando flujos de barro, ríos, áreas con potencial de inundación, esto ayuda a la visualizar mejor la amenaza en un determinado espacio geográfico, donde se intenta modelar el área de afectación por caída de cenizas de acuerdo a los vientos predominantes, para el caso del volcán Irazú, considerando lo que se sucedió entre 1963-1965.

Geografía de la percepción

Cuando se emprenden los estudios espaciales de una termina área es importante combinar la ayuda que proporciona las nuevas herramientas (SIG-GPS), con otras metodologías para abordar el tema amenaza y vulnerabilidades de nuestras comunidades una muy utilizada por nuestro equipo es la geografía de la percepción, donde las comunidades elaboran croquis de cómo perciben la amenaza en sus espacios comunitarios, con ello se logra una mayor sensibilización y capacitación de la importancia de sistematizar las experiencias de las áreas afectadas por emergencias y desastres.

Vemos como el aprovechamiento de la experiencia comunitaria y establecimiento del conjunto de escenarios de amenazas, vulnerabilidades y fortalezas de la comunidad en su territorio, se puede hacer con la aplicación de métodos sencillos para la recolección de información.

Posteriormente en el laboratorio es posible comparar los mapas generados por las comunidades con los mapas generados por los técnicos y científicos, es increíble las similitudes que hay y quizás lo más importante, se logra que las personas tome conciencia de sus problemas espaciales y busque de alguna forma soluciones, porque nosotros podríamos tener unas soluciones muy grosas en nuestras oficinas, pero en realidad los vecinos que viven en una determinada área son los que deben responder de primero ante una emergencia o incidente.

Conclusiones:

Finalmente, los Sistemas de Información Geográfica han alcanzado tal desarrollo al día de hoy, que logran fácilmente hacer sobrepuestas de diversas coberturas (relieve, cobertura boscosa, usos de la tierra, geología estructural y formaciones geológicas, geomorfología, redes (drenaje, vial, cableado, de cajeros automáticos, estaciones de servicio, etc), tipos de suelo, ubicación de sismos, hidrantes, automóviles, temas sociales como por ejemplo tipo de viviendas, ingresos promedio por familia, expediente electrónico de pacientes, ubicación de patronos) facilitando la geo-interpretación, que a su vez pueden también ser representadas en 3 dimensiones, para asemejar más al mundo real. O bien, sus coberturas pueden emigrar hacia otros programas especializados para construir modelos, por ejemplo, el programa *Capra-gis*, donde los datos de ayudarían a construir los archivos .ame necesarios para el modelaje del riesgo.

Contribuyendo a la toma de decisiones en cuanto al ordenamiento territorial y a la planificación del paisaje ecológico se refiere.

Seguridad cibernética: una necesidad mundial

Celso Gamboa Sánchez

Las tecnologías de la información y la comunicación se han vuelto en todo el mundo un instrumento fundamental para el quehacer diario, al punto de que el ser humano ha ido dejando de lado todos los papeles y tiene la información en sus equipos informáticos. La base de la ciberseguridad del Estado son las telecomunicaciones.

En Costa Rica la seguridad de las telecomunicaciones estaba desprotegida, incluso no se ha pensado en asignar un presupuesto para que las oficinas brinden seguridad cibernética a las entidades estatales. Esto se presta para que algunas empresas que tiene información de los ciudadanos como DATUM o TELETEC: lo que hacen es compilar toda la información de ustedes contenida en las bases públicas y venderla. Un dato en DATUM vale alrededor de 5000 ó 7000 colones y es una empresa que al menos tiene 5000 ingresos al día por lo que pueden facturar una suma considerable.

Todos estos datos privados han emigrado de las bases públicas a las manos de una persona muy inteligente que logró hacer un programa que le brinde respuesta al ciudadano, en las bases de DATUM sale si usted ha tenido juicios prendarios o hipotecarios. Los ciudadanos que han luchado por ser excluidos de estas bases quedan totalmente

sacrificados y anulados porque a la hora que van a pedir un préstamo para comprarse un carro o una casa tienen que ir a suplicar que los incluyan nuevamente en estas bases porque son personas, empresas que monopolizan la información.

En el año 2006 Costa Rica empieza sufrir en un ataque cibernético a la banca, logran sacar más de 9 millones de dólares en menos de 6 meses, asumiendo el costo parte del Estado y parte de la banca privada. Del año de 1995 al año 2006 todo lo que se han robado en vehículos, en asaltos a casas y a bancos no alcanza a la mitad de lo que se robaron por Internet, esa es la importancia de la seguridad de un sistema de información.

La cooperación intersectorial

Cómo le vamos a vender a las empresas transnacionales a Costa Rica como un lugar para que vengan a invetir cuando tenemos un sistema de telecomunicación altamente inseguro y lo peor sin un equipo de respuesta para realizar las transacciones seguras de manera oficial.

Dadas las crecientes amenazas a los sistemas y estructuras de información esenciales se debió abordar el tema de la cooperación intersectorial (Conferencia OEA julio 2003). Además del compromiso de identificar y combatir las amenazas terroristas emergentes, tales como las amenazas a la seguridad cibernética. (Declaración de Montevideo, enero 2004). En estas conferencias se decide llevar adelante una estrategia interamericana integral para combatir las amenazas a la seguridad cibernética. En la reunión de expertos Canadá marzo 2004 se recomendó la creación de una cultura mundial de seguridad cibernética y la protección de las infraestructuras de información esenciales. Resoluciones 55/65, 56/21, 57/239, 58/199. Asamblea General de Naciones Unidas.

A raíz de esto en la Organización de Estados Americanos se crea el concepto de CSIRT ya es un concepto viejo es un acrónimo en Inglés se llama CSIRT en Costa Rica porque internacionalmente se obliga a utilizar este acrónimo para estar afiliado a la red internacional de CSIRT, que es un equipo de respuesta a los incidentes de seguridad cibernética. También se implementó en Nicaragua,

Guatemala, en Perú, Salvador, Panamá, países donde habíamos enfocado todas las armas del narcotráfico, la delincuencia organizada.

CSIRT: del inglés: *"Computer security incident response team"*. En su tradución al castellano significa:*"Equipo de respuesta ante incidentes de seguridad cibernetica"*. Nació en la Organización de los Estados Americanos. Su objetivo principal es incorporar el sistema de seguridad cibernética y tecnologías de la información a la protección de la sociedad como un factor minimizador de riesgos y amenazas cibernéticas.

El CSIRT es un equipo técnico compuesto por 60 personas desde ingenieros hasta policías que ejecutan un sin número de labores, para ver la aparición de estas amenazas en las actuaciones no solo de prevención sino también de represión y en este sentido Paraguay, Panamá y Guatemala estan copiando nuestro modelo, están tomando el CSIRT de Costa Rica como parámetro de acción. A que quiero llegar, no es que el CSIRT se encuentra fuera de la esfera judicial porque se ha considerado necesario reprimir unas actividades en contra de la seguridad cibernética no solamente en prevención que es lo que se hace en estos países.

En Costa Rica sí se ha legislado en este tipo de temas, por ejemplo tenemos el delito de la violación de las telecomunicaciones y el sabotaje informático, que sirve como resorte para el Ministerio Público para reprimir estas conductas y como el monopolio de ejercer la ley penal en Costa Rica recae en la Fiscalía, el Poder Ejecutivo traslada otra responsabilidad de seguridad al Poder Judicial, el cual no tiene nada que ver con seguridad del Estado, sino que reprime otras conductas que ya están y resuelve otra clase de conflictos; la seguridad del Estado recae propiamente en lo que es Poder Ejecutivo y en quienes hacen políticas de persecución criminal como la Asamblea Legislativa que el Poder Judicial aplica.

Contribuir con la seguridad y defensa del espacio cibernético costarricense es la visión de este organismo para el desarrollo y modernización del país. Procura incluir el de la *soberanía cibernética*, recuerden que ejercemos control sobre nuestro territorio, sobre nuestros mares, sobre nuestro espacio aéreo pero…y ¿sobre nuestro espacio de Internet?

Han pensado en ese gran espacio que tiene Costa Rica donde se dan todas las conversaciones desde servidores costarricenses, donde se efectúan miles y miles de transacciones a través del espacio informático. Esta visión es la que incluye a Costa Rica como un país integrado, globalizado en un solo circuito y que debemos empezar a proteger. No puede estar siendo invadido, afectado por un grupo de personas que se dedica a terrorismo o a la delincuencia. Costa Rica no es un país con objetos de conquista, no es una potencia, y además no tiene ejército, por eso no ha sufrido todavía un ataque terrorista a las redes de Internet, pero más grave aún que un ataque terrorista y así se puede interpretar son los ataques a nuestras redes de comunicación.

Hoy día por el abandono de la cultura cibernética que tenemos los ticos, ha hecho que incurramos en malas prácticas y que nuestro espacio cibernético se encuentre plagado de un sin número de amenazas. El ejemplo más claro es cuando va a comprar una computadora voy a una empresa a comprar la computadora pero el muchacho me dice que si le pago de contado me la da con el Word y con el Excel instalados y la licencia no se sabe donde quedó, esto convierte a las computadoras en sistemas frágiles, que están expuestos a software maliciosos y dañinos. Nuestras computadoras están repletas de basura y sin que nos demos cuenta las están transformado en robots de otras computadoras.

La misión del CSIRT es llevar a cabo medidas represivas y preventivas de amenazas de seguridad cibernética contra las tecnologías de información y comunicación de Costa Rica, siendo un órgano de actuación inmediata que colaborará con el desarrollo nacional."

Algunos objetivos del CSIRT

- Adoptar estrategias integrales para combatir amenazas a la seguridad cibernética.
- Asegurar el uso de los recursos tecnológicos de información y comunicación en el estado.
- Contar con una entidad que responda a incidentes de seguridad en el campo de las tecnologías de información y seguridad de las comunicaciones.
- Promover una cultura de seguridad cibernética.

Tiene algunos objetivos como adoptar una estrategia integral. Periódicamente nos reunimos con los departamentos de TI de todas las instituciones estatales y no estatales que tengan algún tipo de injerencia en la actividad económica del país para instaurar protocolos ante cualquier situación que pueda presentar una amenaza para la empresa y ante el tráfico normal de las telecomunicaciones del país.

También aseguramos el uso de las tecnologías de la información y comunicación en el Estado, técnicamente esto sería posible cuando tengamos un equipo de respuesta que nos diera la información inmediata de lo que estaba pasando con las telecomunicaciones del Estado, ahora con la apertura vamos a empezar a sufrir el mismo problema de Guatemala y otros países en donde empresas privadas que ofrecen los servicios de telecomunicaciones, abandonando toda responsabilidad con la Superintendencia de Telecomunicaciones, mantiene la privacidad de sus clientes como un plus, como un atractivo más para que compré el servicio y se mantenga en el anonimato que por eso la gran cantidad de secuestros que sufre Guatemala no son resueltos con prontitud porque los proveedores de servicio no tienen comunicación directa con los CSIRT y por pretender proteger la privacidad de los datos hacen que fallen los sistemas de seguridad y que se pierdan segundos valiosos.

Como no se había pensado que las telecomunicaciones se podían usar para robar no había un equipo de respuesta en el ICE, donde usted pudiera llegar a pedir la información, se pasaba de ventanilla en ventanilla y se perdían 12 horas, ahora hay un canal directo para obtener esa información.

Contar con una entidad que responda a incidentes de seguridad en el campo de las tecnologías de información y seguridad de las comunicaciones, es decir el CSIRT es esa entidad que responde a eventos de seguridad y que se ha convertido en un requisito para empresas transnacionales para establecerse en algunos países.

Promueve una cultura de seguridad cibernética, el CSIRT da charlas de seguridad cibernética sobre todo los ingenieros en las empresas públicas y privadas que se señalen para enfrentar situaciones amenazantes para la empresa y a la vez se da un canal directo entre el CSIRT y cada empresa mediante un punto de contacto.

Situación actual

Los incidentes de seguridad cibernética son atendidos por la Unidad de Fraudes del Ministerio Público que a su vez coordina con la Unidad de Delitos Informáticos del Organismo de Investigación Judicial. Recuerden que en Costa Rica la Dirección de la Policía y la Dirección del OIJ la tiene la Fiscalía General.

Eventos presentados

1. Estafas a residentes norteamericanos mediante "operación sorteos fraudulentos" a través de una plataforma computacional desde Costa Rica se hicieron llamadas a residentes de los Estados Unidos y se realizaron estafas superiores a cien mil dólares.

Se hizo un operativo en Costa Rica y se desarticuló una banda criminal. ¿Cómo funciona esto? Se hacían llamadas desde Costa Rica a personas jubiladas y se les decía que habían ganado un sorteo con un premio de tanto, en el identificador salía el número de la junta de sorteos de Estados Unidos, el teléfono era oficial. Se les decía a las personas que para darles el premio libre de impuestos tenían que depositar entre 15 mil o 20 mil dólares. Lo que llama la atención es como desde Costa Rica se comienzan a dar ataques hacia el mundo, como empezamos con tecnología nuestra y con cerebros nuestros a utilizar la tecnología para atacar; no hay países pequeños para este tipo de ataques.

2. El *phising* bancario red criminal compuesta por miembros de Rusia, Rumania, Holanda, Colombia y Costa Rica se apoderan de las claves bancarias y realizan transferencias de fondos no autorizadas, su objetivo "el internet banking". Al 15 de agosto de 2007 en Costa Rica se encontraban estafando un promedio de 8000 dólares diarios. Lograron estafar un aproximado a 135.000 dólares solo en Costa Rica.

¿Por qué personas de Colombia, Rusia y Rumania? Porque logramos detectar que las direcciones IP de donde se hacían estas transacciones se hacían desde sus computadoras. Una persona en Rumania logró meterse a la computadora de Celso Gamboa aquí en San Francisco de Dos Ríos esto pasaba porque posiblemente Celso Gamboa tenía un sistema operativo sin licencia y un antivirus gratis que bajó de Internet.

Los investigadores privados pueden ver las actividades de las parejas por Internet; ahora con cierto tipo de teléfonos yo podría programarlos para ver lo que usted tiene en su correo, no lo hago porque no traigo el equipo y además estaría cometiendo un delito a menos que ustedes den su autorización.

También con los teléfonos de TDMA se pueden duplicar los mensajes de texto; hay gente que transmite información personal vital por mensaje de texto. Hasta esta dimensión están llegando las telecomunicaciones, dentro del porcentaje de intercepción de mensajes de texto en Costa Rica, el 100% ha sido parejas que quieren saber que está haciendo la contraparte.

En el Poder Judicial hemos logrado detectar como están violentando nuestro *firewall*; que siempre lo he dicho no sirve para nada, se apoderan de los números de patrimonio de todas las computadoras de la institución, el patrimonio es una plaquita que dice el número del bien y a quién está asignado, sí la computadora 2021 esta asignada a Francisco D'allanese yo puedo entrar en esa computadora y apoderarme de todo lo que está haciendo, ese robo tiene una trascendencia muy importante para el Poder Judicial. Lo logramos detectar, lo que hicimos fue cambiar todos los números de patrimonio, pasar un antivirus con licencia y crear una red de emergencia para las personas que tienen puestos trascendentales de toma de decisión dentro de la institución para que en sus computadoras se minimice ese riesgo.

3. "Fraude telefónico" *hackers* sudafricanos procedieron a ingresar de manera no autorizada al sistema informático de una empresa a la cual durante 3 horas la trasladaron la facturación telefónica de varias comunidades de Etiopía a dicha empresa cargando el costo al ICE facturando casi 160 millones de colones, solo en 3 horas.

Ese evento no fue fácil detectarlo, fue un trabajo complejo, que no se había hecho ni siquiera en España. Aquí en Costa Rica empezamos en 2006 sin saber que pasaba, llegamos a tener casi 500 denuncias, nadie sabía que era lo que pasaba hasta que nos dedicamos a hacer prueba y error, y llegamos a un modelo que ahora sirve internacionalmente para desarticular las bandas dedicadas al

phising bancario y que ha hecho que el CSIRT Costa Rica se posicione como un CSIRT fuerte por lo menos a nivel latinoamericano. Fueron con *hackers* surafricanos que facturaron cientos de millones de colones, suma que lógicamente rechazaba la empresa, era una empresa muy fuerte tenían más de 700 empleados en Costa Rica dijeron que pagaban la suma pero que inmediatamente se iban de nuestro país.

¿Qué era lo que había pasado? Una empresa surafricana había contratado un *hacker* para que desviara su facturación a otro servidor, resulta que el *firewall* de la empresa x no logra detener al *hacker*, y este logra su objetivo, se dan tres incidentes más, en uno el ICE asumió el costo y otras tres están en litigio.

Debido a la magnitud de ese evento y que Sudáfrica no cuenta con un CSIRT tuvimos que viajar a África, establecer relaciones con la policía del lugar y llegar a pedir casi que por favor a los *hackers* que dejarán atacar a Costa Rica, porque no existía un CSIRT, para celebrar el convenio de cooperación internacional; duramos 7 meses mientras tanto ellos seguían impunemente trasladando facturación a Costa Rica a 7 empresas que eran las que tenían la magnitud para asumir esos impulsos. Ahora no tenemos relaciones con Sudáfrica pero tenemos relaciones con el CSIRT de Estados Unidos que nos hace el enlace directo con África y en 20 minutos podemos cortar la comunicación.

Costa Rica estaba haciendo atacada desde Argentina, se pasa la información del CSIRT a CSIRT y en 12 horas la policía Argentina llegó a la casa del *hacker* que estaba atacando en Costa Rica, por carta rogatoria hubiera durado dos años tiempo risible, creó que es un nivel de respuesta sumamente eficiente, por supuesto que falta muchísimo en cibernética, en Costa Rica no hay una especialización que quisiéramos, somos un país pequeño y pobre.

Ventajas del CSIRT

- El CSIRT labora bajo la modalidad 24/7 los 365 días del año.
- Los CSIRT gubernamentales comparten e identifican las amenazas trasladando la información a sus homólogos en segundos.

- Los CSIRT gubernamentales protegen la "soberanía cibernética del país".
- Los CSIRT son un "plus" altamente valorado por las empresas para realizar inversiones.

¿Qué ventajas le dio esto ha Costa Rica? Ahora cada vez que Costa Rica solicita una información a otro CSIRT en cuestión de minutos ya se tiene la información con total confianza, al punto de que el departamento de Defensa de los Estado Unidos que ntes no compartía información con nadie, a pesar de que Costa Rica da y da ellos no comparten información, pero ahora ya están compartiendo con nosotros.

¿Por qué en Estados Unidos? porque hoy están los servidores de correo de yahoo y de g-mail de donde se están enviando los correos. Hay un sin número de detalles que luego podemos conversar de la informática forense de cómo se puede desarticular una banda, aunque lo hagan con direcciones de correo falsas, en un café Internet lejos de la casa, siempre hay un rastro que nos lleva a la persona culpable.

Las ventajas trabajamos 24 horas los 7 días de la semana. Los CSIRT gubernamentales comparten e identifican las amenazas trasladando la información a sus homólogos en segundos. Los CSIRT gubernamentales protegen la "soberanía cibernética del país". Los CSIRT son un "plus" altamente valorado por las empresas para realizar inversiones.

Público meta

- Se encuentra dirigido a proteger infraestructura crítica del gobierno y su sistema financiero.
- Sistema Bancario.
- Telecomunicaciones.
- Poder Legislativo, Ejecutivo y Judicial.
- TSE.

Tiene un público meta por supuesto se encuentra dirigido a proteger infraestructura crítica del gobierno y su sistema financiero al sistema bancario, las telecomunicaciones, el Poder Legislativo, Ejecutivo y Judicial y el Tribunal Supremo de Elecciones.

Necesidades del CSIRT por supuesto vamos a necesitar infraestructura, *hardware, software*, personal profesional, certificación internacional. Ya la certificación nacional la tiene Costa Rica.

En la infraestructura ustedes no van a encontrar un CSIRT Costa Rica, son un grupo de agentes que tengo en la sección de fraudes, es un grupo de personas del Ministerio de la Presidencia, un grupo de ingenieros, personas profesionales. Debería estar una persona 24 horas en una oficina para atender al público como cualquier oficina del Estado, por la labor que hemos hecho de contención por los beneficios que hemos dado al estado, pero no se le ha tomado la importancia por la misma falta de conocimiento de los legisladores y por el abandono del Poder Ejecutivo de esa labor de prevención recargado en el Poder Judicial, sin embargo igual alguien debe hacer algo por este país.

El último incidente de importancia que se reportó en nuestro país fue con los *chips* de los teléfonos celulares donde personas sin la autorización de un juez con un cierto equipo pueden clonar el chip de sus teléfonos celulares para que puedan escuchar sus conversaciones; el servicio se está dando en la calle a un precio de 150 dólares más o menos, lo que hemos detectado en este momento en Costa Rica por los esposos y las esposas infieles, pero se puede dar para espionaje vean lo que pasó con lo del TLC y el memorándum famoso como se están revelando cosas por la falta de seguridad en Costa Rica.

Capítulo 7

Protección de redes

Vulnerabilidades de los sistemas

Jorge Blanco Incer

Si usted cree que la tecnología puede resolver sus problemas de seguridad, entonces ni conoce usted sus problemas ni sabe de tecnología.

"Secretos y Mentiras", Bruce Schneier

En el área que coordino se reciben las denuncias del OIJ, por delitos informáticos, anteriormente se tramitaban varias por mes, actualmente se tramitan varias por día. Este aumento se debe a que ahora se cuenta con distintos medios de transporte: xDSL, Wi Max, 3G; que puedo utilizar para realizar cosas positivas y no tan positivas.

¿Cómo proteger?

Inicio con una frase del señor Bruce Schneier que es todo un gurú en el tema de seguridad la cual indica: "Si usted cree que la tecnología puede resolver sus problemas de seguridad, usted no conoce sus problemas, ni conoce la tecnología".

Después de esa frase nos quedamos un poco pensativos en el sentido de, ahora que hacemos. La idea que tiene uno es solventar este tipo de problemas de seguridad, colocando algún *hardware*, o cualquier elemento de red que nos ayude a solucionar cualquier intrusión

en nuestros sistemas o nuestras redes, pero ya vemos como no es tan simple, más adelante trataré de explicar cómo podríamos solucionar este tipo de problemas.

¿Contra qué proteger?

La Asociación de Control del Fraude (CFCA), realizó una encuesta en 16 países, a diferentes compañías, un 80% de estas compañías indicó, que las pérdidas que ellas tenían por fraude habían incrementado y el 45% manifestó que habían visto incrementar el fraude dentro de las mismas compañías. Entonces se observa que estos ataques, no solo proviene desde el exterior, sino que dentro de nuestra compañía podemos enfrentar este tipo de situación.

Muchas veces yo diseño mi sistema de protección para proteger mi intranet, suponiendo que los ataques provienen desde la Internet, de esa forma tengo una cierta protección en forma ideal, pero ya vemos que hoy en día van incrementando los ataques que tengo dentro de mi propia red.

Se probó un exploid que salió para *Windows Vista,* el mismo se generaba mediante *broadcast,* de un total de 10 máquinas, afecto a 8, máquinas que supuestamente estaban protegidas, con todos los sistemas de seguridad, contra los ataques, sin embargo resultaron afectadas. La prueba se realizó sin dar aviso a los usuarios, por lo que algunos perdieron información. Hay que analizar el costo de este tipo de ataques: ¿cuánto es lo que afecta a mi empresa? En ese sentido yo tengo que ver qué tipo de acciones debo tomar.

Fraudes

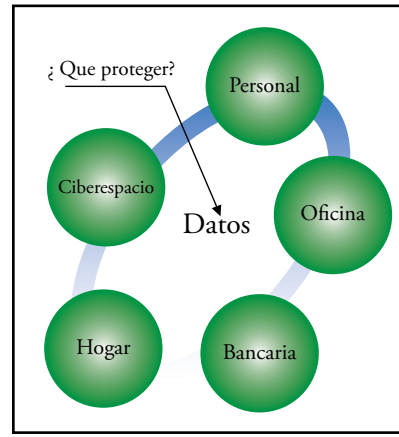
Normalmente ese tipo de ataques están orientados a realizar algún tipo de fraude. Buscan obtener satisfacción por violar sistemas. Estos se denomina *hackers*, que por lo general no buscan tomar partido ilícito de ello sino como por satisfacción personal.

Están otros que aprovechan esta vulnerabilidad de las redes, buscando obtener beneficios, por lo general económicos, derivados de este accionar, sin embargo ambas causan daño.

¿Qué proteger?

Y decimos ya que van a causar daños ¿qué van a proteger? ó ¿qué y cómo proteger?

Muchos opinan que el valor solo lo puede dar la persona que ha sido afectada, si yo a nivel monetario tengo -por darles un ejemplo- 100 millones de colones y pierdo un millón de colones, la representatividad no es tanto. Pero si tengo cien mil colones y perdí esos cien mil colones, perdí todo mi capital. De tal forma que solo la persona que se ve afectada puede dar valor a la pérdida.



¿Qué tengo que proteger?
¿Qué tipo de información tengo que proteger?

En teoría, se debería de proteger todo aquello que está conectado a la red, pero hasta cierto punto, dado que actualmente en el mercado, encuentro diferentes dispositivos que se conectan a la red.

Por ejemplo, un refrigerador inteligente, que ayuda a ahorrar energía, tiene una pantalla conectada a cámaras, que muestra el interior, mediante las cuáles decidir si se toma algo del interior o no, evitando que abra la puerta por un periodo extenso de tiempo. Este dispositivo se conecta a Internet para realizar pedidos, en forma automática. En nuestro país, el sitio *amidomicilio.com* ofrece este tipo de servicios, para estos dispositivos.

También están las lavadoras que cuentan con la tecnología *Smart – Tabs* las cuáles, mediante la conexión a Internet, me envían un mensaje de correo indicándome que la ropa ya está lavada. Hace unos meses salieron al mercado unos robots que limpian la casa, los cuáles, mediante conexión Wi Fi, me van informando las áreas de la casa que han limpiado. Todo este tipo de dispositivos están

conectados a Internet los estoy utilizando en mi propia casa, nada más lo tenemos que configurar, dentro de poco tiempo, cuando se busque una asistente para la casa, entre los requerimientos habrá: que le gusten los niños, que duerma en la casa, y que sea CCNA, de lo contrario, no va poder configurar todos estos nuevos dispositivos que utilizo en mi casa, para ejecutar las tareas del día a día.

¿Contra qué?

Contra qué usualmente hay que proteger. Inicialmente el correo electrónico era donde mandan más tipos de ataques, sin embargo, actualmente los sitios web, han tomado mayor ponderación.

China es el lugar donde hospedan más programas nocivos con el 80% del total, seguida por Estados Unidos, los Países Bajos y Alemania, en estos sitios es donde se encuentra la mayor cantidad de afectaciones.

Por el momento vemos que China tiene sus ataques centralizados a nivel interno. En general lo importante es que no se puede contabilizar cuántos de estos han sido exitosos, si es que fueron efectivos.

Por otro lado está lo que nosotros recibimos en el correo

Este es un dato del 2009 del *Spam*, casi un 90% del correo que nosotros recibimos en el 2009 es correo basura. En el ICE se están utilizando varios métodos, para poder superar este tipo de ataques de *spam*, sin embargo siempre existen, se disminuyen, pero no se pueden eliminar.

El *Phising*, es la técnica de suplantación de identidad, a nivel de páginas web, para que el usuario suministre datos personales. Este tipo de ataques se ha venido disminuyendo, pero aún se presentan casos.

Los que están más afectados son *PayPal y e – Bay*, son las entidades, que a nivel mundial tienen mayor presencia, sin embargo también hay bancos, y redes sociales que se están viendo afectadas.

Se tiene que para el 2008, América Latina ocupaba el sexto lugar como fuente de *Spam*, pero como nos vamos superando cada vez más, llegamos a ocupar el segundo lugar en el 2009.

La publicidad es lo que más se manda como *Spam*, paso de televisión y de medios escritos a Internet, de esta forma se detecta un poco más el crecimiento, aquí se puede decir que tal vez la crisis contribuyó a este cambio.

Entonces, la tecnología no nos puede ayudar tanto, o si ponemos equipos a nivel de *hardware* ¿por qué es que ocurren estas cosas?

Las personas que administran las redes, los ingenieros en sistemas, los ingenieros electricistas, no siempre entienden lo que está pasando realmente. Sin embargo como tenemos ingenio, le decimos que la culpa no es nuestra es de otros, muchas veces revisamos las tareas con receta, muchas veces se sigue una receta para eliminar algún problema, para eliminar algún tipo de inconveniente, pero que pasa si la tecnología que nosotros estamos aplicando no trabaja como nosotros esperábamos.

¿Sabemos qué hacer?, ¿sabemos tomar las decisiones correctas en nuestra red para solventar esta situación?, ese es uno de los problemas que se nos presenta.

¿Por qué ocurre?

Otro problema es que la infraestructura de red que se conecta, la infraestructura de red que se adquiere, no siempre está orientada a la intención que tiene la empresa. No es lo mismo ser administrador de un banco, que una empresa de telecomunicaciones o algún otro tipo de negocio.

La Inter conectividad que nosotros damos debe estar orientada a la misión de la empresa que nos contrató, a la visión de la empresa para la cual estamos laborando, dado que si el *hardware* o el equipo que nosotros administramos falla, también hay un file dentro de la empresa.

Tenemos que pensar bien todos los procedimientos, pensar bien las políticas que vamos a implementar, el análisis de los riesgos, ¿Qué pasa si desconecto este equipo? ¿Que falta para solventar un ataque?, sí afecto la imagen de la empresa, no solo voy a perder a nivel

económico, el problema de imagen afecta seriamente el quehacer diario de la empresa.

Debo tener bien claro hasta donde llego yo como administrador, hasta donde no, muchas veces a los TI o a los administradores los buscan para todo, mira quiero conectar esta impresora, tal cosa no puedo hacer, no puedo imprimir, etc. Entonces hay que delimitar bastante claramente el trabajo que nosotros vamos a desempeñar.

Muchas veces nos centramos en los detalles olvidando la generalidad, nos perdemos en el que hacer que tenemos que ejecutar, los detalles son importantes pero solo cuando es necesario, tenemos que tener siempre una imagen del trabajo que nosotros vamos a desempeñar, no dejarle todo a la parte de tecnología.

En la mayoría de los casos, el administrador hereda la red, él no fue el que la implementó, él no fue el que la diseñó, si no que llegan a una empresa cuando la red ya existe y a muy pocos se les enseña a analizar, a desarrollar y a desempeñar estas redes.

Cuando ocurre una avería lo principal es la disponibilidad de servicio, ¿Cómo recuperar la red en el menor tiempo posible?, puede ser que los equipos fueron configurados en forma remota y así los adquirimos, en esa configuración y así continúan. En otros casos, cuando iniciamos labores, algunos componentes ya están bajo un ataque, puede no ser masivo, ni puede ser obvio, pero siempre están siendo atacadas y permanecerán siendo atacadas sino hacemos cambios.

Por lo tanto hay que hacer una documentación correcta de esa red para detectar ese tipo de inconvenientes, este tipo de problemas y solucionar los mismos.

Por último, confiamos mucho en la tecnología, sabemos que tenemos la tecnología en nuestras redes y por lo general nos despreocupamos, depositamos erróneamente en la tecnología la confianza y nos olvidamos del riesgo que puede tener la empresa.

Es importante conocer la tecnología, no solo poner la tecnología en nuestras redes, sino conocer hasta que niveles podemos llegar y utilizar métodos sistemáticos para llegar a los puntos finales que

queremos solventar, para disminuir las afectaciones que tenemos en nuestras redes.

Con esto concluyo, como les dije al inicio, no es solo la tecnología la que nos va a resolver los problemas, sino también, las personas, teniendo un correcto seguimiento y aplicación de estos conocimientos, de la tecnología que vamos a implementar en cada una de nuestras redes.

Conociendo a tu enemigo

Richard Elizondo Giangiulio

En muchas ocasiones se utiliza el término seguridad informática, sin embargo, el concepto que mejor se adapta a las necesidades de hoy en día es seguridad de la información ya que este involucra todos los ámbitos de la computación y la relevancia de la información para su dueño. El resguardo de la información es lo realmente importante ya que el resto de componentes de una red pueden ser recuperados (equipos, computadoras, sistemas, etc.), sin embrago, si la información se pierde todos los elementos de la red dejan de tener importancia.

Seguridad de la información

La seguridad de la información tiene tres pilares fundamentales que son integridad, confidencialidad y disponibilidad, los cuales proporcionan un marco para la protección de la misma.

Integridad

Garantiza que no existan cambios no aprobados en la información.

Confidencialidad

Garantiza que la información está disponible únicamente para quien esté autorizado para acceder a esta.

Disponibilidad

Garantiza que la información se encuentre a disposición de quienes deben acceder a ella en el momento que se necesite.

Adicionalmente a los tres pilares de la seguridad de la información existen otros factores que afectan el proceso de protección. Estos factores ya sean externos o internos modifican la estrategia de protección de la información.

Estos factores son llamados "El Entorno" y las compañías están sujetas, a proteger la información no solo porque es valiosa por sí misma, sino porque existen regulaciones que deben ser acatadas.

En Costa Rica existen leyes que regulan aspectos relacionados con la seguridad de la información. También se han creado entidades como la Superintendencia de Telecomunicaciones (SUTEL), que posee regulaciones sobre cómo los proveedores de servicios de telecomunicaciones deben proteger la información de sus clientes. Otro claro ejemplo es el de la Contraloría General de la República (CGR), la cual establece que las empresas estatales deben acatar un conjunto de normas en materia de seguridad de la información.

Por otra parte las empresas poseen objetivos organizacionales que se ven reflejados en las políticas organizacionales y las de aceptación de riesgo, las cuales tienen como finalidad normar el comportamiento de los usuarios y establecer responsabilidades ante una fuga o pérdida de información, estableciendo la criticidad con base en el tipo de información involucrada en el evento.

Por ejemplo una política organizacional puede establecer que el uso de redes sociales y los servicios de mensajería instantánea estén restringidos.

Adicionalmente, las empresas deben estar concientes de las consecuencias en el diseño de las estrategias de protección de la información y asumir los riesgos que estas presentan. Para esto debe existir una política clara de aceptación de riesgos definida previamente.

Proceso de protección

A menudo confiamos en el nivel de seguridad que hemos implementado en nuestros sistemas, ya que tenemos un software de antivirus, hemos actualizado nuestro sistema operativo instalando las últimas actualizaciones disponibles, sin embargo, en cualquier momento pueden aparecer ataques que aprovechen vulnerabilidades aun no detectadas en nuestro sistema y por lo tanto ya no confiamos en nuestro nivel de seguridad.

Lo que sucede hoy en día es que aparecen múltiples ataques diariamente que provocan que el proceso de protección tenga que ser una tarea constante con el fin tener un nivel de seguridad confiable.

Defensa en profundidad

El modelo de defensa en profundidad o seguridad en capas funciona colocando barreras en cada una de las diversas capas con el fin de prevenir una violación a la seguridad, siendo la capa de datos la más protegida de todas.

Física

Es la primera capa y la más tangible, corresponde a todos aquellos mecanismos destinados a proteger físicamente la infraestructura, los sistemas y los datos.

Entre estos mecanismos se encuentran los sensores de proximidad para el acceso a las áreas restringidas, las cámaras de vigilancia, cerraduras, alarmas contra incendio, plantas de suministro eléctrico UPS's y aires acondicionados.

Red

Es la segunda capa e involucra desde los cables hasta dispositivos como *firewalls, IDS's, IPS's,* los cuales están diseñados para proteger la infraestructura.

Los *IPS*'s o preventores de intrusos permiten detectar un ataque o un comportamiento anormal y ejecutar una acción con base en reglas previamente definidas y el comportamiento normal del tráfico de red.

Los *IDS's* o detectores de intrusos permiten detectar un ataque y ejecutar una acción predeterminada.

Los *Firewalls* son dispositivos para filtrar paquetes por medio de direcciones IP origen y destino y los puertos o servicios que se desean permitir o bloquear.

Los *switches* proporcionan un nivel adicional de seguridad en la red permitiendo separar los dominios de colisión y mantener la privacidad del intercambio de datos entre los involucrados.

Infraestructura

Es la tercera capa e involucra servidores, computadoras, periféricos y sistemas operativos.

Entre las acciones indispensables para proteger la infraestructura se encuentran los procesos de aseguramiento de los sistemas operativos y su oportuno parcheo y actualización.

Lo anterior con el fin de eliminar las vulnerabilidades de los sistemas operativos y deshabilitar los servicios o funcionalidades que no se estén utilizando y evitar o minimizar las posibilidades de una violación a la seguridad.

Aplicaciones

Es la cuarta capa y corresponde a las aplicaciones que se utilizan en nuestros sistemas.

El desarrollo de las aplicaciones debe ser controlado en términos de versiones, con lo cual debemos conocer en cuál versión estamos operando, cuál fue la última versión estable.

Es importante controlar la entrada y la salida de datos de la aplicación para no permitir valores que no sean los esperados.

La separación de los ambientes de producción y de desarrollo es fundamental para la protección de la información ya que la manipulación de

los datos en ambientes de producción solamente debe ser realizada por los mecanismos autorizados.

En el proceso de desarrollo de las aplicaciones se debe mantener una separación de tareas para que las personas que realizan el desarrollo no sean las mismas que prueben las aplicaciones y tampoco las que administran las bases de datos, ya que si todas estas tareas las realiza la misma persona no podríamos confiar en la aplicación desarrollada.

Adicionalmente, el control de acceso a la aplicación es un factor crítico en el proceso de protección de la información ya que nos permite identificar a los usuarios y darles solamente los privilegios necesarios para realizar sus labores.

Debemos recordar que la simplicidad es una de las mejores técnicas para mantener el control y la seguridad de las aplicaciones.

Datos

Es la quinta capa y pretende proteger los datos de manera que solamente quienes estén autorizados para trabajar con ellos puedan hacerlo.

Encripción es uno de los mecanismos para proteger los datos, de esta forma si estos son sustraídos de nuestros sistemas no podrán ser utilizados.

Redundancia es un factor crítico de éxito para proteger los datos y mantener disponible y segura la información contenida en los sistemas críticos.

Conociendo a tu enemigo

Es primordial conocer a quien nos enfrentamos y cuál es el perfil de nuestros enemigos. Existen tres categorías de atacantes actualmente reconocidas.

El *Script Kiddie*: El 95% de los atacantes se encuentran en esta categoría, son personas que intentan vulnerar algún sistema o tratar de ganar acceso utilizando aplicaciones disponibles en la red de manera gratuita para realizar un ataque sin objetivo definido. No tienen el conocimiento de lo que están haciendo, solamente lo hacen por diversión.

El atacante habilidoso: Utiliza las mismas herramientas que el *Script Kiddie* con la diferencia que este si tiene el conocimiento de las acciones que está realizando. Persigue un objetivo específico con el fin de obtener un beneficio.

El atacante interno: Es una persona de confianza que posee los privilegios, tiene conocimiento de los sistemas y acceso autorizado a estos. También persigue un objetivo específico con el fin de obtener un beneficio.

¿Cómo protegernos?

Para protegernos contra el *Script Kiddie* y el atacante habilidoso, usualmente se colocan *firewalls*, detectores de intrusos, *software* de antivirus y *antispam*, así como una estrategia de defensa en profundidad.

El caso del atacante interno es completamente diferente pues adicionalmente a los mecanismos tecnológicos se deben crear políticas para prevenir que esta persona se vea tentada a cometer un fraude, y en el caso de que suceda, pueda ser detectado y sancionado.

Tipos de ataques

Existen múltiples ataques y técnicas para tratar de vulnerar los sistemas y esto hace que las labores para la protección de la información sean trabajo de todos los días.

No existe una medida única para proteger las redes y equipos, todo se basa en una estrategia de defensa en profundidad, entre más capas implemente mayor será el nivel de protección.

La implementación de estrategias de defensa en profundidad puede desalentar al atacante y lograr nuestro objetivo primordial, proteger la información de nuestros sistemas.

Por último debemos recordar que la seguridad trasciende la tecnología, no es tecnología, la seguridad es concientización y un estilo de vida.

Seguridad del ciberespacio

Jonathan Solano González

Tratamos el tema de la ciberseguridad, desde una perspectiva sistémica, ya que día a día las empresas, sus sistemas de información y sus redes están enfrentando una variedad de amenazas de seguridad que incluyen, fraudes asistido por computadores, espionaje, sabotaje, vandalismo, incendios, terrorismo, virus, troyanos, *Hacking* de computadores, negaciones de servicio con niveles cada vez más ambiciosos y sofisticados.

En primer lugar las empresas y los usuarios de computadoras deben conocer cuál es su exposición de riesgo, posteriormente deben crear una política integral con acuerdos de confidencialidad entre patronos y colaboradores.

Debe existir una verdadera clasificación de la información en información pública, privada o secreta. Las empresas deben garantizar las tres características principales para la seguridad de la información: Integridad + Disponibilidad + Confiabilidad. De igual forma se requieren de las tecnologías adecuadas para proteger las redes y sistemas.

Estadísticamente se muestra a nivel mundial que solo el 20 % de estos incidentes son provocados por personas externas a una organización.

El medio más utilizado por estos es la Internet, la cual es aprovechada para lanzar ataques con un sin fin de objetivos que van desde pura diversión hasta convertir esta actividad en un negocio lucrativo.

Las redes están pobladas de usuarios maliciosos o desconformes, piratas informáticos, creadores de virus, saboteadores de información y de programas responsables de que el 80 % de los incidentes de seguridad sean ocasionados por el personal interno de las empresas.

Actualmente no existe una estadística nacional con registros de estos eventos que muestren la realidad total de nuestro país. Hay esfuerzos por parte de la Universidad de Costa Rica - PROSIC (Programa para la sociedad de la información y el conocimiento) con ayuda de otros entes que tienen participación en estadísticas y los índices de incidentes en Ciberseguridad en Costa Rica.

Esto se atribuye a que el sector financiero es uno de los campos más afectados por este tipo de actividad, existe una línea muy delgada entre el "Riesgo de Imagen" ante la sociedad costarricense y la apertura de entes financieros en revelar como sus vulnerabilidades fueron explotadas. En los últimos 5 años, bancos públicos y privados de primer orden en Costa Rica han sufrido este tipo de delito. Se podría decir que la seguridad como materia académica no existe, la seguridad es tan abstracta como hablar del amor, del hambre, etc.

Un nuevo campo de acción

Las nuevas tendencias o las nuevas tecnologías ofrecen un nuevo campo de acción, si bien es cierto vivimos en la era de la información, ya pasamos la era industrial, salimos de la era agropecuaria y ahora la Internet nos brinda una zona horaria veinticuatro por siete, sin fronteras, mientras nosotros dormimos, "los chinitos" están despiertos, que son uno de los mayores productores de *hackers* que existen a nivel mundial, por el lado de América tenemos a los brasileños, con un buen nivel y podemos decir que la seguridad es una profesión completa, es una herramienta que es utilizada para medir a nivel nacional o a nivel internacional ciertos sectores, como la seguridad

civil, seguridad personal. Se puede hablar de miles de aspectos de la seguridad, por eso se dice que la seguridad es algo abstracto.

El componente base de la información es el dato, la información es una sucesión de datos, esta sucesión de datos podrá tener diferentes interpretaciones, a partir de la subjetividad se pone un valor a la información de lo que hay en los intereses de cada quien; una base de datos del poder judicial gustaría mucho tenerla, para saber aspectos como direcciones, registro civil, cédulas información que se clasifica ya como pública y como privada. Al tener estos datos, ahora la información como tal es un activo de valor para las empresas, si bien es cierto uno de los recursos importantes es la parte del recurso humano, peor que tal la información que va dentro de ese recurso humano.

La seguridad informática, utiliza los medios computacionales, la parte que decimos de toda la plataforma tecnológica, vamos a concebir que necesita ser adecuadamente protegida, ahora más adelante vamos a ver a que se refiere eso de "adecuadamente"; donde se encuentra, decir que es la interrelación, dentro de la información las personas que lo utilizan, los equipos que las soportan deberían estar adecuadamente "seguras".

Actualmente los sistemas financieros, transnacionales y corporaciones son los que han tomado la iniciativa de proteger el activo información con presupuestos adecuados para el desarrollo de metodologías, políticas, planes de capacitación, mejores prácticas y equipamiento técnico como IPS (Sistemas Preventivos de Intrusos), Paredes de fuego (*Firewall*), Antivirus, Filtrados de contenido para navegación en Internet, programas AntiSpam, Redes Virtuales Privadas (VPN), Encripción de datos, etc.

Sin embargo la mayor debilidad en todas las empresas es lograr una cultura de seguridad preventiva, ya que de nada vale importantes inversiones cuando todavía existe una negligencia corporativa en cumplir con dichas políticas.

Por eso es constante encontrar en nuestras auditorias y pruebas de *hackeo ético* vulnerabilidades provocadas por descuidos de los

administradores de redes, sistemas, en los usuarios finales es muy común escucharlos compartir contraseñas de validación para aplicaciones las cuales han permitido tomar control de sus redes y sus equipos, y posteriormente son entregas en informes para sus correcciones.

¿Qué protege la seguridad informática?

Tiene tres características principales, la confidencialidad, la integridad y la disponibilidad de la información, se dice que la información puede existir de muchas formas, no es únicamente lo que se ve en un computador es también lo que se manda en fax, lo que se imprime, una agenda; cualquier esfuerzo que haga una organización por implementar seguridad informática es obsoleta, una negligencia corporativa, a veces se es muy negligente en la tenencia de información.

Cuando se habla de confidencialidad de la información se habla de la necesidad de la información para el acceso a las personas, todavía se mantienen las estadísticas en el 80-20 80%; los incidentes de seguridad son internos y 20% son externos. La mayoría del tiempo los incidentes internos son por el exceso de confianza, robo de información, pasos mal dados, niveles otorgados en bases de datos, usuarios que no es el administrador de la base de datos, ahí es donde vienen los problemas cuando hay descuido, puede ser que un usuario mafioso este sacando la información. La protección es muy difícil ahora con todos los recursos informáticos. ¡Quién no puede hacer copy-paste y mandarlo al correo de otra persona! Hay que darle importancia a las medidas que se tomen con respecto al robo de la información.

La integridad: los datos no deben ser alterados y la disponibilidad es que la información este disponible siempre que se necesita. Son los tres elementos principales de la seguridad informática, hay otros más pero la esencia está en esos tres.

Algunas de las maneras en que la información puede sufrir daños en términos de un emisor a un receptor, pueden ser por medio de la interrupción, de la modificación o de la alteración de los datos; hay muchos ejemplos de las anteriores.

La seguridad informática procesa o soporta procesos complejos, por ende las empresas los necesitan para mantener un alto flujo competitivo o la imagen comercial, hace unos pocos días ustedes se dieron cuenta que un Banco Estatal, ya han sido varias veces donde se pusieron los archivos en los EEUU en la página web, el impacto que puede tener eso si esto cae en los medios de comunicación masiva, con todo el sensacionalismo, donde el golpe o el impacto comercial puede ser muy fuerte, hasta provocar el descalabro financiero, el cierre bancario, por la mala interpretación de sus páginas web, donde un *hacker,* un muchacho puso la foto del gerente general con cachos, no tiene ningún golpe en sus datos, así una travesura puede provocar, si se incluyen los medios de comunicación masiva puede acarrear una histeria colectiva, esto prueba que los sistemas del banco son inseguros; que riesgoso es, bueno ahora vamos a ver algunas estadísticas de que los sectores financieros son los más golpeados, ¿porqué? por qué lucrativamente a mi me iría mejor trabajando en "el lado oscuro de la fuerza" cobrando trescientos dólares por archivo capturado, que haciendo una consultoría, ciertamente es más lucrativo.

¿Internet? Es el producto caliente de la guerra fría, después de la segunda guerra mundial, esto avivó un poco más para que las universidades en Estados Unidos comenzaran a crear una red, después tenía entre comillas lo que era ampliación del intelecto humano, desde 1972 se llama Internet, ahí comienza a explotarse el nombre de Internet y se considera que en 1983 nace verdaderamente Internet, esto fue resultado de la milicia y todas los principales líderes en EEUU cuando necesitaban compartir información podían disfrazar su ampliación del intelecto humano y dio como resultado la mayor red de información de todos los siglos.

Ahora existe Internet. Desde mi punto de vista, es una vía pública, ustedes circulan por la vía, en la parte vial. Es responsabilidad de las empresa si van a proteger sus entradas y salidas, tan es así que vivimos en el ciberespacio y nos quedamos sin la debida protección ya que solo es conceptualizado como algo virtual.

Internet es una zona peligrosa

Internet como lo dije es una zona peligrosa, yo le llamo la gran red, y la gran red está poblada de tribus y piratas informáticos, cuando hablo de tribus cibernéticas es por que todavía estamos en la prehistoria, yo todavía trato de visualizar un poco más lo que es tecnología y siento que todavía estoy en la prehistoria, estamos empezando a vivir en la era del ciberespacio y todos esos conceptos, la parte de marcos normativos jurídicos no están preparados para tipificar algunos de estos delitos tan es así que se tuvo que dejar libre al muchacho que clono la página de tres bancos privados, que lo que estaba haciendo era *fishing,* capturando los passwords, que le permitían tener el usuario y el password y la entrada a la fuente.

Lo que les decía, la explosión del ciberespacio ahorita, es para mí como el viejo oeste, todavía andamos con pistolas y ciertamente se están haciendo los esfuerzos por normativas internacionales, normativas locales para detener un poco esto; pero si bien es cierto todavía la mal intención o los malversados que quieren utilizar la parte de la red para cometer sus delitos, pues todavía tienen una cabeza de gato, eso por que todavía la seguridad informática es como un ratón, todavía le falta bastante, ahora lo vamos a ver en las estadísticas.

En el comercio igualmente en la red va a ser mucho más grande que las transacciones de lo que se da en Internet, porque son billones de dólares ahora más bien se dice que la empresa que no este en Internet con su página web publicada va a perder un poco el campo de acción de sus servicios.

La parte de las bases de datos, los sistemas operativos, la capa de aplicaciones, la capa de los procesos tienen que ver con la seguridad de la información y una de las capas más difíciles la capa de los usuarios, es difícil trabajar con una cultura de seguridad dentro de una empresa, o sea manejar o llegar a tener la seguridad en su negocio, es un proceso cíclico, que deberá cumplir con cada adversidad para tener los controles y objetivos para llegar a lo que es un sistema de gestión de seguridad informática; cada organización es diferente.

Para poder contar con un sistema de madurez de seguridad se debería empezar con lo que es la evaluación de la información, pocos conocen dentro de sus empresas cuánto vale la información que está en la bases de datos, ¿cuánto vale la información?, poniendo un precio a la información, si es confidencial, si es privada, si es pública, las empresas ya la tienen clasificada, ya saben que compartir, que niveles de acceso dar.

El gran error de las compañías a parte de dejar la seguridad para lo último, es pensar en el negocio, hay que dar eventos, hay que despachar el producto lo más rápido posible, hay que ofrecer un producto ágil, aquí es donde viene la seguridad informática, ahora asociar la parte de concesión, costo, utilidad tiene todo un trabajo bastante laborioso si no se consiguió desde el principio del proyecto.

Después de la evaluación se debe hacer un análisis de riesgo, conocen los trabajadores el riesgo residual que existe entre sus empresas o la aceptación del riesgo, igualmente al salir Internet, se está expuesto a otros riesgos, ¿existen los controles adecuados o no? Luego de este análisis de riesgo, hay que tener identificadas varias soluciones tácticas, operativas y técnicas.

Debe existir una concientización de entrenamiento, tener un ciclo de auditoria y monitoreo, eso es importante, y debería existir lo que es un plan de contingencia. Pues esto es un ciclo interesante que debería cumplirse para llegar a una etapa de madurez con respecto a la seguridad informática; cuando hablábamos de aspectos tácticos, operativos y técnicos, lo táctico que es un marco normativo, un marco normativo en todo lo que son políticas, estándares, guías, procedimientos, la jurisprudencia que se tenga, la legislación con la que cuenta un país, está el tema de firma digital, y por ende seguir trayendo o dando pase o inicios de nuevas conceptualizaciones de tecnologías.

Desde la necesidad de una nueva tipificación en la legislación judicial para declarar el delito informático y sus diferentes formas y castigos, hasta crear unidades especializadas en el sector gobierno para desarrollar programas de capacitación a estudiantes los cuales

desde tempranas horas deben conocer como se debe manejar o clasificar la información personal, privada y pública y cómo prevenir ser objeto del robo de identidad, perdida de bienes, fraude por tarjeta, el uso de internet en niños es aprovechado por pederastas para obtener direcciones, teléfonos o citas a ciegas.

Un verdadero SGSI

Las organizaciones deben conseguir con la seguridad de la información, obtener en un verdadero SGSI "Sistemas de Gestión de la Seguridad informática" que contemple todos los ámbitos lógicos y físicos de los sistemas de TI, organizacionales y seguridad contextual. Con respecto al tipo de amenazas, pueden ser, humanas, físicas, lógicas o informáticas, en cuanto a amenazas humanas hablábamos de *hackers*, de *craquers*, del personal interno, de terroristas de ingeniería social, dentro de las redes, etc.; las amenazas físicas, los desastres naturales, la seguridad de laptops, lo que puede valer un disco duro, la información que puede contener; amenazas lógicas algunos *software*, la negación del servicio; todo ello entendido desde la esfera pública y la privada.

Hay que tener una serie de precauciones para evitar todas las amenazas, borrar cualquier rastro que uno puede dejar, para que no se pueda seguir la información, crear una puerta trasera que sirva de apoyo para cualquier eventualidad. Para protegerse de algo más agresivo como lo son los *craquers*, siempre van con la mala intención de crear la negación del servicio, entrar a cierta identidad, botar la página web y anular el correo electrónico.

Se presentan una serie de estadísticas, pertinentes a las tecnologías de la información y a sus niveles de uso y actividades ilícitas en Costa Rica. Hay que rescatar que el ciberespacio es el campo de acción que únicamente va a depender de la mente que lo utilice, la información es pública, si se quiere fabricar una bomba los elementos para la fabricación se consiguen en la red, los humanos somos los que decidimos como utilizar ese tipo de acción. Por ejemplo si logran acceder a las bases de datos del Poder Judicial (hachear las bases de datos), imaginen que van en carro, y ven a una muchacha

que les gusta en otro carro, nada más se fijan en el número de placa y pueden tener su dirección, nombre, número telefónico, estado civil y etc.; todo eso considerado como información privada.

Antes de desechar un equipo informático hay que borrar de forma permanente la información personal. Se debe tener un protocolo de desecho, rómpanlo, denle un martillazo, como quieran pero no olviden la parte de destruir sus almacenamientos, ya sea óptico, magnético, etc. Compruebe que un sitio web es seguro y estable, saber lo que es el *¡hashing t t p!* o sea que tiene un nivel de certificado digital.

Usen contraseñas seguras y tengan todas las precauciones al utilizarlas, y esto que va más al lado de las empresas tener a una persona encargada de la seguridad de la información; la figura del oficial de la seguridad informática o auditor informático, es muy importante destinar recursos a la parte de seguridad informática. Aplique la administración de recursos humanos así como de proveedores y socios de confianza normas del mismo nivel de seguridad que utiliza en sus sistemas informáticos, desde el gerente general hasta usuario más simple.

Para nadie es un secreto que las bases de datos son buscadas por todo tipo de negocios para ofrecer desde tarjetas de crédito, combos vacacionales, promociones, etc. Con este tipo de información pueden clasificar a personas y empresas según sea su capacidad de adquisición. Buscan Información pública que sea registrada en el padrón electoral, información crediticia de bancos y línea blanca, información de bienes, direcciones, teléfonos, participación en sociedades anónimas o empresas, información salarial y en algunos casos hasta la foto de la persona es brindada por este lucrativo negocio.

Se dedican en brindar esta información a financieras, Bancos, cooperativas, puestos de Bolsa, etc., los cuales investigan a sus nuevos clientes con el fin de validar o descartar si la personas están involucradas en casos jurídicos o más.

Soluciones para prevenir las estafas y los fraudes

Jairo Villalobos Salas

SmartSoft apoya a instituciones y conglomerados financieros en la detección, lavado de dinero y prevención del fraude bancario, a través de la incorporación de sofisticadas tecnologías como: sistemas expertos, árboles de decisión y redes neuronales que permiten revisar y analizar el comportamiento transaccional de los clientes, facilitando la toma de decisiones y la ejecución de un conjunto de acciones automáticas.

Básicamente somos una empresa que trabaja como proveedores para las empresas financieras de soluciones para prevenir las estafas y los fraudes. Agregando a estas soluciones tecnologías de avanzada, sistema de neuronas y el árbol de comportamientos.

Nuestros sistemas se han ubicado en diferentes instituciones Comcel Banco Ripley, un Banco de Chile, que está dedicado a atender una tienda en específico, trabajos más formales como es el Banco INBURSA, bancos como BAC, procesadoras de crédito como Credomatic y bancos grandes en América del Sur como el Guayaquil que es uno de los bancos más grandes del Ecuador.

Algunas cifras disponibles

En el 2006 las pérdidas por fraude y clonación de tarjetas fueron de 2.6 billones de dólares, aquí estamos concentrados en una parte muy específica que son las tarjetas de crédito y de debito, pero la cantidad de dinero suelto que esta por ahí es una cantidad enorme. Igual las pérdidas por transacciones en línea están arriba de los 3 billones de dólares. El fraude de tarjetas esta cerca de 1.8 billones de dólares.

En el 2007 aumentó cerca de un 43% , en el 2008 aumento un 22% y en Estados Unidos se vieron afectados cerca de 9 millones de personas; cuando vemos todos estos datos la gente se asusta pero esta es la realidad que tenemos y el problema que enfrentamos.

El *phising* como todos saben es un fraude social muy difícil de combatir. Algunos timos para comprometer la información a través del *phising*, algunos muy conocidos fueron el *City Bank*, el Banco Nacional (la vivimos casi todos en Costa Rica) y por ahí hubo muchos otros, que pedían todos los datos disque para actualizarlos en donde había que incluir la calve personal y otros datos personales.

Otras formas un poco más personales: a este se le dice el "fraude romántico", porque es de 1 a 1 en puntos de venta, que es cuando la terminal que tiene el comercio sufre algún tipo de alteraciones que permite copiar muy pocas tarjetas pero por lo general es muy buena la selección; por ejemplo: el uso de pescadores es algo que cualquiera puede tener en un bolsillo, que al pasar la tarjeta por ahí se copia toda la información, incluso hay pescadores más sencillos, mucho más pequeños que comparados con el tamaño estándar de una tarjeta son mucho más pequeños. Por ejemplo acá en Costa Rica se utilizan mucho como son los casos de restaurantes, en gasolineras se han capturado muchos datos, es como lo más usado.

En ATM: cajeros automáticos que tiene un lector que para abrir la puerta hay que pasar la tarjeta y si no, no abren. Los que no tienen eso básicamente lo que están haciendo es leyendo la tarjeta, aquí en Costa Rica hay muchos de estos que no tiene el lector, muchos de estos son sofisticados tienen transmisores incluso pueden transmitir la información encriptada. Por ejemplo en Brasil se estaba pasando

por ahí información y los bancos no podían saber que era lo que estaba pasando, se encriptaba la información se pasaba a una laptop a 300 metros y nunca se pudo saber cuáles tarjetas habían sido leídas como tal. En los cajeros se ponen teclados falsos que capturan claves y aunque ustedes no lo crean funciona. Existe una tecnología donde se instala una camarita y se pueden ver los datos que se digitan y aparte si tiene un aparatito como estos lee toda la información que está en la banda magnética de la tarjeta.

Algunas otras técnicas de sobra conocidas son el *pharming,* los *keyloggers*,*virus, spyware, malware y niffers*. Varias técnicas combinadas para vulnerar sistemas financieros y obtener bases de datos completas. Técnicas digitales como los *Keyloggers* que son los programitas que se instalan en la computadora y toman toda la información y la reenvían. Estos programas lo que buscan es accesar a bases de datos grandes.

Respuesta del sector Financiero:

- Mejorar los mecanismos de seguridad de los productos financieros (CHIP).
- Fortalecer los controles de acceso y seguridad de cara al cliente.
- Monitoreo de comportamientos inusuales en clientes, comercios, canales.
- Incorporación de estándares como el *PCI* (Payment Card Industry).

¿Qué ha hecho el sector financiero? Básicamente son situaciones de mejoras por ejemplo banco *ITAUNO*, bancos muy grandes en Brasil, *BANCOMER* uno de los bancos más grandes, *BANMEX* en México, todos estos hacen miles de transacciones por día, por lo que todas sus tarjetas están en chips, en teoría estas tarjetas son inclonables, aunque usted tenga la información del chip.

También ha fortalecido los controles de la seguridad, lo cual a veces complica a los clientes pero son medidas que funcionan. Además el monitoreo de comportamientos inusuales que aquí es donde estamos un poco más nosotros, básicamente son herramientas para detectar que un cliente no hacía algo pero ahora lo está haciendo, no acostumbra ir

a un cajero pero ahora lo está haciendo, no compraba en el extranjero pero ahora lo está haciendo. Por otra parte está la incorporación de estándares como el *PCI* que es uno de los estándares más conocidos, que básicamente es un conjunto de normas que todas las instituciones de crédito deben cumplir, que tiene que ver con la seguridad perimetral, el *firewall*, la encripción de datos, etc.

El sector financiero mundial es una de las industrias que más invierte en seguridad. Aún así los sistemas informáticos más "seguros" han sido vulnerados. En este tema el sector financiero es el que más invierte, incluso en algunos países supera al gubernamental. Bajo la consigna de que cualquier sistema puede ser vulnerado, desde los más buenos hasta los más sencillos, se ha generado el lineamiento de hacer la información "inservible", encriptando los canales y bases de datos de inicio a fin. Básicamente lo que se busca es hacer la base inservible, esa es la tendencia y es la experiencia que tenemos como empresa, hacer la data inservible muchos piensan encriptar como lo hace *PCI* de punto a punto, otros piensan en hacer mezclas, como los bancos con las claves dinámicas y ese tipo de cosas.

Por ejemplo *Heartland* estaba certificado por *PCI* y no lograron evitar el ataque, una entidad externa preparada para esto y entran a sus datos, es de asustarse. Se trata de un certificado digital pagado por el banco x, y, z, de 100 mil dólares al año, le atacaron el *DNS* caché; aquí no hay *spyware*, no hay *norton* que detecte este tipo de *phising*, porque es un tipo no detectable, es algo por debajo que si le cambia al usuario final, el sistema simplemente no se da cuenta.

Finalmente está el uso del *DNSSEC* es un estándar que hace tiempo está disponible, la intención de todo esto es tratar de prevenir los problemas de seguridad. Esto es algo que no es solo a nivel transaccional, es vital para el sistema y es importante ver que aunque esto se cataloga como una vulnerabilidad, un *DNS* envenenado es incapaz de prevenir este tipo de ataques. En realidad *DNSSEC* utiliza el *TKI* normal pero no entran las entidades certificadoras, a pesar de que *Verizans* si está participando con el *ITAN* para implementar la solución, pero en el proceso como tal no hay ningún certificado. Para lo que nos va servir es para garantizar de alguna forma la respuesta

de los *DNS*, esté funcionando de extremo a extremo y hasta que todo esté firmado y la gente tenga un servidor que soporte *DNSSEC* no va a funcionar. En resumen es una ayuda pero no es la solución total. Esta es una vulnerabilidad que afecta toda la estabilidad del sistema, sin embargo, es la primera que se encuentra en 15 años, por lo que el sistema es bastante estable, no creó que se encuentre otra en mucho tiempo.

Capítulo 8

Protección de equipos

Cómo proteger los equipos

Luis Diego Espinoza Sánchez

Lo primero que debemos determinar que es lo que vamos a proteger, cuánto vale la información personal, podemos comenzar con lo de cada uno. ¿Cómo vamos a proteger esa información?, ¿Qué medidas tomamos para proteger la información? ¿Quién o qué es la amenaza?

Información valiosa

Dónde este la información valiosa es lo que debemos proteger, entonces es importante que si bien tenemos que hablar de computadoras y la amenaza cibernética, también tenemos que tomar en cuenta la parte física y la parte social.

¿Quién nos va a defender?... ¿La tecnología? No sé. ¿Dónde guardamos la información valiosa? ¿Dónde guardamos la clave del banco? cada uno puede analizar esto; a lo mejor en un *post-it* a la par de la computadora o en la parte de atrás de la agenda ó la escribe en un archivo de texto en la computadora y la guardan. ¿Dónde guardan la clave del banco?

¿Qué información personal damos a ese montón de encuestas para participar en una rifa? Le damos números, le damos los 4 últimos

dígitos de la tarjeta de crédito, le damos dirección, teléfonos, e-mail, cuánta información personal damos voluntariamente, con los ganchitos de la rifa. ¿Qué hacemos con los estados de cuenta? Los tenemos o los archivamos, pero después de un año, …pum a la basura, lo sé porque justo a la par de mi casa hay un tarro de la basura, entonces van llegando a mi casa los estados de cuenta de los vecinos, los *boucher*, todo llega ahí y completitos se ven las compras, el número de tarjeta, todo. Todos esos son elementos son cotidianos y no tiene que ver exactamente con tecnología.

Amenazas

Las posibles amenazas que podemos tener. TR/Fraudpack.sxa, ese es un *spyware* que encontré ayer, uno que no detectó McAfee, no la detectó ni la última versión más actualizada, y se arruinó en la maquina.

¿Esa es la amenaza? o ¿*Microsoft Windows* es la amenaza? ¿los *hackers*? Hay un porcentaje grande malicioso donde están los *hackers* ó ¿Es Internet el problema? ¿El técnico que revisa la computadora? ¿Nosotros mismos? Ya no sería una amenaza sería una debilidad, esas son cosas que debemos analizar.

Proteger equipos ayuda

Para proteger los equipos, ya pensando propiamente en la tecnología que manejamos; el antivirus, el *antispyware, el firewall* personal ayuda, si, los parches de *Windows*, ayudan bastante, el mejor experto en seguridad chequeando mi computadora, también ayuda, pero todo puede fallar porque tenemos muchas cosas activas, en nuestras computadoras, antivirus y siempre nos caen virus y siempre perdemos la información. Quiere decir que no es un asunto tan tecnológico, que tiene que ver con muchos otros elementos también.

Proteger la red o protegerse de la red

Con respecto a proteger la red, o protegerse de la red, podemos darnos una idea de lo que esto significa con solo ver el porcentaje de inversión que se hace en seguridad informática desde grandes industrias, desde grandes corporaciones hasta nivel personal. Mucha gente no paga su licencia antivirus, su licencia *antispyware* o su

suscripción anual. Es importante determinar cuánto representa todo lo que se invierte en *software* y en *hardware*, principalmente porque para poder correr la última versión del antivirus, necesito ponerle más memoria a la máquina, así lo demanda el antivirus que estoy instalando.

Tenemos navegadores que no nos dejan navegar, que nos bloquean todos los sistemas de red, porque el *firewall* no lo autoriza, pero… es este un mal necesario ¿hasta donde podremos llegar con este asunto? Hasta que colapsemos completamente, cuando una computadora muy básica no pueda trabajar, no pueda procesar los datos, bueno esto es un asunto que tenemos que evitar.

La mejor solución será estar desconectado ¿quién podría estar desconectado hoy en día? ¿Quién puede sobrevivir sin correo, sin *Skype*, sin *Messenger*, sin *Facebook*, sin ese tipo de cosas? Son muy pocas las personas que yo conozco que pueden sobrevivir sin esto. Pero el asunto de estar desconectado no pierde validez, de hecho de las mejores prácticas de las empresas que firman certificados digitales, el servidor que contiene las llaves privadas tiene que estar desconectado de la red para poder firmar los certificados digitales.

¿Cuánto cuesta la seguridad?

¿Cuánto cuesta la seguridad? La gente que trabaja aquí en las compañías dando ese servicio nos pueden hablar un poco de eso. La cuota del mercado en seguridad alcanzó los 13 mil millones de dólares americanos en el 2008. Imagínense el negocio que hay detrás de esto, hay un crecimiento del 18,6% con respecto al 2007, principalmente por un asunto de acceso seguro al e-mail. El asunto del *spam* y los correos electrónicos se ha vuelto todo un problema desde hace unos años para acá. Obviamente la respuesta es y del lado de las compañías que ofrecen esos servicios, el crecimiento en la venta o suscripción de los *software* para protegernos, en los *firewalls,* en las cajas, es una cantidad de productos que nos venden; al rato pienso que si no tendrán algo que ver esas compañías con todos los problemas de virus y de tecnología que tenemos… pero bueno digamos que no.

Toda esa tecnología no nos puede proteger de cosas como el *phishing,* la compañía, la universidad o la empresa pueden tener un

ultra mega *firewall* de última generación que cuesta $100 000, con un *súper mega software* de un súper antivirus, *antispyware* que pagó para toda la institución y así tener los parches de último momento; toda esa inversión que hizo la organización al final para algo tan simple como el *phising* no sirve, así de simple, el *phising* es una palabra combinada de *password* y *fishing* que significa pesca de *passwords*. Por qué voluntariamente le entregamos toda la información a otra persona.

Voy a contar una anécdota que ha sido el incidente más interesante que he enfrentado, tal vez no de muchísimo impacto, pero si interesante porque me hirió en lo profundo porque un servidor que yo había instalado fue *hackeado*, entonces me sentí herido, me dedique a averiguar que era lo que había pasado, *hackearon* un servidor muy sofisticado por cierto el que sabe de redes sabe que tal vez el TSP / IP funciona con puertos, un puerto web, uno los servidores los protege para que no todos los puertos estén abiertos, sino solo los que se utilizan para el servicio que se brinda. En la nueva versión de IP, que es IP6 los puertos son distintos, entonces fue algo muy hábil porque venían disfrazados dentro del paquete de IP versión 4, paquetes de IP versión 6, accesando un servicio en un puerto IP de los que yo tenía bloqueados. Modificaron la página web, redireccionaron la página y comenzaron a mandar correos a clientes de eBay, para que accesaran su cuenta, muy fino el trabajo, solamente te mostraban la página de login, para que digitará su usuario y *password* y lo redireccionaba a la página verdadera de eBay y seguía funcionando normalmente o sea una vez que le daban sus credenciales va directo a eBay. Lo que hacía era que capturaba usuarios y *passwords* de eBay. Esto lo siguió la FBI y la Interpol, según entendí se robaron cerca de $200 000.

¿Cómo proteger al usuario de él mismo?

¿Cómo proteger al usuario del mismo? bueno esto es una cosa compleja y no solo tiene que ver la tecnología. Debemos crear conciencia, malicia y educar; esto requiere toda una estrategia hay que invertir recursos en esta área, parte de los dineros que se destinan para comprar cajas de seguridad deberían dedicarse a educar y

concientizar a la gente, con seminarios, talleres. Charlas con demostraciones muy simples, para que la gente se de cuenta a que tipo de cosas están expuestas, a que clase de horrores pueden cometer los *hackers* o hacer evidente que clase de errores comete la gente al dar ese tipo de información, eso podría ser una buena práctica. La gente que se dedica al asunto de la seguridad, la SER, la NIS, las agencias de seguridad constantemente mantienen información y se mantienen alertando a las organizaciones sobre los eventuales problemas.

Pérdida de datos, ¿cuánto cuesta perder datos?

Un caso interesante de agosto del 2008, 40 millones de tarjeta de debito y crédito de diferentes vendedores fueron robados con una técnica que se llama *wardriving* la cual consiste en andar con una laptop con una antenita inalámbrica detectando redes inalámbricas con *software* especial que permite saber si esa red está abierta para entrar, incluso si no esta abierta la inclusión del IBP es simple quebrarlo, es muy fácil meterse y encontrar en uno de los bancos una red abierta y por ahí se metieron. De hecho es muy interesante yo lo he hecho por diversión, va uno en el carro por la calle y la computadora va detectando un montón de redes y además se le pone un GPS y le hace un mapita de las redes que están abiertas, esto es el *wardriving* pero más allá de un juego, puede ser un problema.

Debemos formar cibernautas que estén alertas que se puedan defender solitos, la gente tiene que desarrollar su propia capacidad de estar alerta, de defenderse para enfrentarse a nuevas situaciones. Todo este asunto de la ingeniería social no se aplica solo a la tecnología, se aplica a muchas otras cosas, por ejemplo en la forma en que se puedo manipular una persona por medio de la información personal que se posee.

¿Por que el tema de formar cibernautas?

Recientemente salió una publicación que señala que el 20 o 25% de los ataques de seguridad son producidos desde adentro, de esos casos, la mitad son intencionales, la otra mitad son por ignorancia, entonces es importante mitigar ese 25%, tal vez mitigarla con información, con educación, para concientizar.

Voluntariamente entregamos la información entregamos un dato sin pensar si quiera si ese dato puede comprometer la información personal o la publicamos en *Facebook*, o en *HI5*. Es impresionante la cantidad de información que se encuentra en las redes sociales. Muchas veces la gente usa como clave el nombre de la mascota, las iniciales de sus hijos, el apodo de este y toda esa información está en *Facebook*, porque es información personal y se encuentra ahí, incluso con esta información se pueden atar cabos, la gente que se dedica a esto puede averiguar los accesos.

El correo electrónico, si lo capturaron lo pueden usar para hacer correos masivos, pero el peligro del correo electrónico no es solo esto, el correo lo utilizamos para nuestra cuenta en *Facebook*, en el banco. Para que la gente no tenga tantas claves y usuarios, se está tratando de unificar, por ejemplo hay una iniciativa de *Google* de utilizar el correo para todo, de manera que yo tengo un solo login para accesar a diferentes servicios, pues entonces si a mí me capturan la cuenta de correo el peligro es severo.

En estos sistemas de servicios públicos, cada vez que usted pierde la clave, la forma de verificación es por correo, entonces si yo tengo acceso al correo electrónico de esa persona ya tengo acceso a todas sus cuentas, de todos los servicios, entonces es más peligroso que el hecho de lo que lo utilice solo para *spam*.

Rol de la tecnología

¿Cuál es el Rol de la tecnología? La tecnología… no podemos vivir sin ella, nos ayuda pero también es costosa y complicada, no es la solución definitiva para protegernos de los ataques, por más caro que sea el antivirus o el *firewall*, puede ser la máxima tecnología, que es una ayuda, si es importante pero no es la solución. También la tecnología facilita el delito, hasta el momento toda esta información de las redes sociales facilita humanamente este asunto de la ingeniería social, para obtener claves, para obtener información personal.

Por otra parte está Gobierno Digital información de los ciudadanos en línea, que interesante resulta que en el Registro Nacional puedo consultar el número de placa de mi carro, pero el número

de placa me devuelve mi nombre completo, el número de cédula y hasta mi dirección. El asunto se vuelve delicado porque tras de eso la consulta esta abierta al público, ya con el número de cédula, es muy fácil conseguir toda la información que se necesita de esa persona para cometer el fraude.

Invertir en seguridad

Invertir en seguridad esto es una frase que me robé por ahí, "las cosas suceden…" por más que invirtamos en seguridad, por más que nos eduquemos, los problemas en seguridad siempre van a haber, "…la seguridad ayuda, pero la seguridad no debe manejar el negocio".

La mejor solución

La mejor solución podría ser una combinación de malicia y de desconfianza empresas como *Microsoft o Linux* no son del todo confiables, también pueden dar problemas. Los procedimientos seguros no solo son un asunto de tecnología, el estado de cuenta que me llega en papel, lo destruyo antes de botarlo, lo destruyo totalmente para que sea un procedimiento seguro.

El uso de *software* con diferentes proveedores, hacer un control cruzado, no usar *software* de un mismo proveedor completamente, a veces es bueno poner a otro a la par para ver como está el asunto. He visto casos con dos antivirus instalados que dan problemas, que los dos se dan duro, que uno dice que el otro no funciona es asunto que tendrán que acomodarse un día, porque no podemos depender tanto de un solo proveedor, combinar cosas el sistema operativo de un fabricante y el *firewall* de otro, eso de que el sistema operativo, el antivirus, el *antispyware* sea todo de un mismo fabricante eso no es tan confiable o conveniente. Soluciones simples pero efectivas eso es lo que hay que buscar, partiendo del punto de que hay que analizar qué es lo que estamos protegiendo.

Malware: Software malicioso

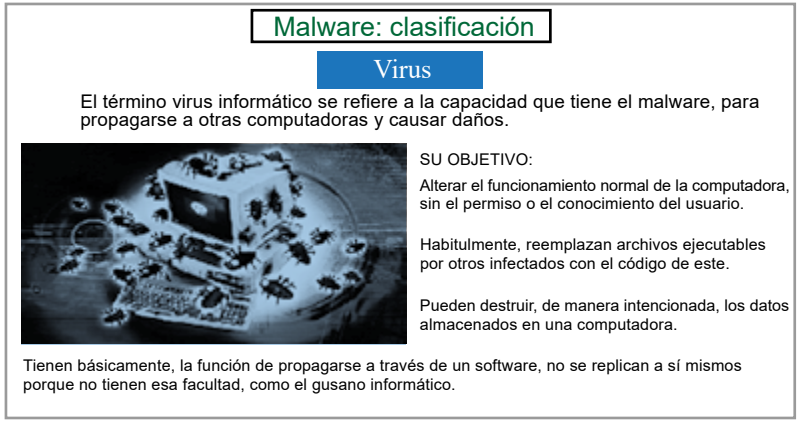
Edgardo Baltodano Xatruch

Malware significa código o software malicioso. Muestra o descarga anuncios publicitarios que aparecen inesperadamente en la computadora, pudiendo hacerlo simultáneamente cuando se está conectado a Internet, o después que se ha instalado en la memoria de la computadora. Su objetivo es infiltrarse en el sistema y dañar nuestra computadora sin que lo sepamos, generalmente se llamaba al *malware* antivirus, pero en realidad el virus es un tipo más de *malware*, pero los *adware,* los *troyanos* y los virus, los gusanos, el *hoaxes*, el *spam,* el *phising*, el *rookit*, el *spyware*.

El *adware* como su nombre lo dice viene de *adverstiment*, de anuncios en inglés y es una muestra o descarga de anuncios publicitarios, nos llega de un momento a otro, aparece cuando estamos trabajando en la computadora, ya sea que estemos navegando en Internet o ya nos hayamos desconectado.Puede ser que algo se bajó de Internet, de un momento a otro se está trabajando y aparece ese un anuncio y usted dice (usuario novato) hay que lindo gratis, aunque no sé portugués pero se entiende que es un protector de pantalla, lindo y gratis, por aquí dice gratis, ahí también dice gratis, entonces damos click aquí y nos empezamos a meter en problemas, ya sea que bajemos

algún *software*, o que nos piden una autorización y ahí nos van llevando a través de ingeniería social y cuando nos damos cuenta estamos entregando nuestros datos; ese es el concepto del *malware.*

Normalmente el *troyano* viene disfrazado de algo inofensivo como un protector de pantalla pero por detrás trae código malicioso que quiere hacerle daño a nuestro equipo y no solo eso, puede abrir un puerto, una puerta trasera, para que desde ahí ya alguien pueda entrar, es decir, se meten a tu casa y abren la puerta de atrás, cualquier persona entra y ni cuenta se esta dando de que alguien esta entrando a su computador.



Virus

El famoso término virus, como lo muestra la imagen anterior tiene la propiedad de propagarse. Además de que es troyano y hacer daño, puede propagarse, buscar puertos para auto enviarse y generar correos. Si se tiene una lista de correos el virus comienza a enviar código malicioso con su nombre, este llega al correo de un amigo que lo abre porque sabe quién es la persona que se lo envía, pero en realidad usted no ha enviado nada, fue el virus el que se encargó de hacerlo.

Gusanos

El término Gusano, proviene de la novela de ciencia ficción *The Shockwave Rider***,** publicada en 1975, y hace referencia a programas capaces de viajar por sí mismos a través de redes para realizar cualquier

actividad una vez alcanzado un computador. Los gusanos informáticos son similares a los virus, pero no dependen de archivos portadores para poder contaminar otros sistemas. Estos pueden modificar el sistema operativo con el fin de auto ejecutarse como parte del proceso de arranque del sistema.

Para contaminar otros sistemas, los gusanos explotan vulnerabilidades o utilizan algún tipo de ingeniería social para engañar a los usuarios y poderse ejecutar. Tiene la propiedad de duplicarse así mismo. Los gusanos son muy similares a los virus, pero el término de donde proviene, ¿Por qué se llaman gusanos? De esa novela se tomó el término para determinar que los gusanos son una especie de *malware* que no necesita de un archivo adjunto para viajar a tu computadora, por medio de un archivo adjunto, mandan un word contaminado, o un correo contaminado. Si su computadora no tiene los parches, el *Windows* actualizado con los últimos parches de seguridad, por ahí se es vulnerable para la injerencia de gusanos y el virus. El gusano tiene la propiedad de duplicarse a sí mismo, se parece mucho al virus, al virus que nos ataca a los humanos.

Del inglés hoax: engaño, broma

Del inglés hoax: engaño o broma, su finalidad es conseguir direcciones de correo o congestionar un servidor. Normalmente una persona conocida recibe una "alarma" de un supuesto virus y nos "hace el favor" de notificarnos para que tomemos precauciones en nuestro equipo. Congestionamos, enviando un montón de correos, cada uno tiene una lista grande de gente en la libreta de direcciones. En realidad no es como un virus, este no causa ningún tipo de daño de su equipo, tienden a congestionar la red. Vean la imagen.

URGENTISIMOOO!!!!
POR FAVOR, HAZ CIRCULAR ESTE AVISO A TUS CONTACTOS!!!
En los próximos días , debes estar atent@: No abras ningún mensaje con un archivo anexo llamado:
Negro en la casa blanca, independientemente de quien te lo envíe... Es un virus que abre **una antorcha olímpica que quema todo el disco duro C** de la computadora. Este virus verndrá de una persona conocida que te tenía en su lista de direcciones...Es por eso que debes enviar este mensaje a todos tus contactos.

Es preferible recibir 25 veces este correo que recibir el virus y abrirlo. **Si recibes el mensaje llamado: negro en la casa blanca, aunque sea enviado por un amigo, no lo abras y apaga tu máquina inmediatamente.** Es el peor virus anunciado por CNN. Un nuevo virus ha sido clasificado por Microsoft como el virus más destructivo que haya existido. Este fue descubierto ayer por la tarde por Mc Afee. Y no hay arreglo aún para esta clase de virus. Este virus destruye simplemente el Sector Zero del Disco Duro, donde la información vital de su función es guardada.

Hay gente que se lo cree, hay quienes se asustan tanto que lo envían a 400 personas y otro por allá hace lo mismo. Este engaño va a llegar de una persona conocida, viene de un amigo que me está advirtiendo a mí, el usuario nos esta haciendo un favor para que tomemos las precauciones, pero en realidad no es nada. Tengan cuidado con eso, no hay un virus que les va a quemar todo el disco duro.

Spam

El Spam toma su nombre del genial grupo cómico inglés Monty Python, en el que la camarera de un restaurante describe los platos del menú a una pareja. Se le llama *spam* a los correos electrónicos basura, que son enviados masivamente a direcciones electrónicas compradas por empresas con la finalidad de vender sus productos. Se refiere a la práctica de enviar e-mails publicitarios no solicitados. Es decir nos están enviando correo no solicitado.

Phising

El *phising* viene del inglés pescar, lo que busca es conseguir información confidencial, vía correo electrónico o página web, con el propósito de que los usuarios de cuentas bancarias contesten el correo para así entrar.

Por ejemplo ponen el logo de la empresa en realidad te hacen creer que algo paso: “Banco de Costa Rica le comunica que con la entrada del año 2007, los servidores de procesos han sido actualizados y están ya operativos. Sin embargo, y a la ingente cantidad de usuarios que utilizan el Internet como medio de pago seguro, nos vemos en la obligación de pedirle una rápida restauración de los datos de las nuevas plataformas”. Suena bonito verdad, suena a banco, continúa: “si no ha entrado en su cuenta bancaria en las últimas horas, se le ruega lo haga de inmediato para evitar cualquier posible anomalía o la futura pérdida de datos”. Y aquí viene el gancho ahora si vamos a pescar ya tire la carnada, y dice así: “puede entrar en su cuenta en el siguiente enlace www.bancobcr.com.”... es el mismo enlace, si ustedes lo leen dice que es el bancobcr.com pero si yo caigo en ese enlace lo que me va a llevar es a una página *gemeliada*. Ahora que está de moda esta palabra, entradas gemeliadas

del partido, las placas gemeliadas; entras a un sitio como el que siempre has visto en tu banco BCR pones tus datos y ya no hay nada que hacer, de hecho es como si entregara la tarjeta con el número de pin.

Rookit

Corresponde a un conjunto de herramientas que permiten el control del usuario *root* y de los procesos del sistema operativo, a la vez que estas aplicaciones permanecen indetectables para el mismo y por ende, para el usuario. Los *rootkits* son programas que son insertados en una computadora después de que algún atacante ha ganado el control de un sistema. Generalmente incluyen funciones para ocultar los rastros del ataque, como es borrar los logos de entradas o encubrir los procesos del atacante. El *root* es como el usuario administrador de una máquina. En lo que consiste es robar el control del usuario *rookit* para a partir de ahí empezar a hacer cosas, por ejemplo: robar información, abrir puertas traseras y otros daños que pueden hacer a las computadoras.

Spyware

Se refiere a programas espía. Recopila información del sistema en el que se encuentran instalados ("husmean" la información que está en nuestro equipo) para luego enviarla a través de Internet, generalmente a alguna empresa de publicidad o en otros casos lo hacen para obtener direcciones de e-mail. Todas estas acciones se enmascaran tras confusas autorizaciones al instalar programas de terceros, por lo que rara vez el usuario es consciente de ello. El *spyware* se refiere a los programas espías que se meten en nuestra red, se roban nuestros códigos, se roban las teclas que usamos.

El Banco Nacional por ejemplo, tiene un sistema de entrada muy bonito -al menos ahora- donde ya no tienes que escribir, hay que escribir en una parte y la otra la hacemos con *mouse* te cambian los números de lugar, no haces *click* en el mismo lugar, entonces esto es excelente para evitar los problemas con los *spyware* y con los *fillover.*

Algunos *malware* famosos que recordamos y que hemos visto en la UCR: *El Chernobyl* ese si dañaba la información, dañaba el sector 0 del disco duro de la información. El virus *Melisssa*, el *I Love You*, que era un correo que mucha gente lo abría por que nunca nadie le había enviado un correo que dijera *I love you*, entonces al abrir ahí activaban un código malicioso, y vamos de nuevo. El código malicioso agarraba los primeros 50 destinatarios de correo y los enviaba, así con cada uno, imagínense lo que mandaba.

El código rojo es básicamente el malware que dañaba servidores, aquí en la UCR no recuerdo si fue el código rojo o con el *blaster*, hace años y no existía ese tipo de organización que tenemos ahora, distribuíamos los antivirus en Cds y era una duplicación de discos para poner los parches para combatir los *blasters* y era toda una situación y era un trabajo terrible.

En la UCR ¿Cómo estamos ahorita? Tenemos un servidor se llama *Control Manager*, trabajamos con las soluciones *Trend Micro*, anteriormente teníamos *Mcaffe.* Tenemos consolas descentralizadas en las unidadades, tenemos una buena cantidad, cada consola descentralizada fiscaliza las máquinas de cada unidad. Por ejemplo, la consola de derecho controla las máquinas de derecho, la consola de economía controla las máquinas de economía. Las consolas descentralizadas bajan las actualizaciones de Internet y las máquinas no viajan a Internet, viajan a la consola descentralizada y es mucho más rápido y cada consola se reporta al *Control Manager*, este es un panorama general de cómo esta el sistema anti *malware* de la UCR.

Malware. 10 recomendaciones para su protección	
	Método de protección
1.	Utilizar una cuenta de usuario con pocos privilegios (no administrador) en su equipo.
2.	Crear una contraseña de alta seguridad.
3.	Cada vez que se transfiera un archivo desde o hacia Internet se debe tener la precaución de revisarlo contra virus.
4.	Se debe comprobar todos y cada uno de almacenamiento de información, soportes ópticos (CDs, DVD, blu-rai) o tarjetas de memoria (SD, MMC, XD, compact flash), que se introduzcan en la computadora.
5.	Comprobar los archivos comprometidos (ZIP, RAR, ACE, CAB, 7z).
6.	Hacer copias de respaldo de programas y documentos importantes, pueden ser guardados en un CD, DVD, entre otors medios externos.
7.	No instalar programas de dudosp origen.
8.	Evitar navegar por sitios potencialmente dañinos, buscando cosas como “pornografía”, “ programas gratis”, “mp3 gratis”, claves, licencias o cracks para los programas comerciales.
9.	Mantener las actualizaciones automáticas activadas, como por ej. el *Windows Update.*
10.	Tener un programa *antivirus, antispyware y un firewall* instalados en su computadora, y mantenerlos actualizados, ya que cada día aparecen nuevas amenazas.

Protege tu familia, tu integridad, tu computadora

Luis Diego Esquivel Herrera

Internet un mundo de oportunidades. Internet es la ventana que nos abre hacia el mundo exterior, nos da la opción de comunicarnos al mundo. Por ejemplo las redes sociales nos dan otra manera de interactuar y esto es muy importante en la educación sobre todo para los niños. Nos permite hacer muchas cosas que cotidianamente hacíamos de forma física: transacciones bancarias, investigación, el compartir archivos, información, música, entretenimiento y otros. Sin embargo, eso conlleva una responsabilidad, debemos utilizar la tecnología de forma adecuada es importante que tener reglas muy claras sobre todo para lo que es la niñez de cómo se debe utilizar la computadora.

Protección en línea versus seguridad en línea

- **Protección:** Debemos proteger nuestras computadoras con tecnología de la misma forma que aseguramos la puerta de la casa.
- **Seguridad:** Debemos actuar de forma tal que podamos protegernos de los riesgos asociados a Internet.

Protección es todo lo que hacemos para que la computadora este segura, es decir usar todos los mecanismos necesarios ya sea antivirus, actualizaciones; la seguridad se entiende como los comportamientos que tenemos nosotros de ser precavidos ante una serie de patrones a los que típicamente no les pondríamos atención pero que nos pueden meter en muchos problemas.

Principales riesgos y amenazas en línea

Si hablamos de computadoras estamos hablando de *virus, gusanos, troyanos y spyware.* Si hablamos de los niños hay muchos tipos de amenazas, cada día surgen nuevas formas de peligros; estamos hablando de *Cyberbullies*: abuso de archivos compartidos, invasión de la privacidad, contenido inquietante y depredadores. A nivel de información personal estamos hablando de fraude informático, engaños, robo de identidad y *spam*. Estas son cosas que solo con conectar la computadora y navegar en Internet estamos expuestos hoy en día.

Principales amenazas de la computadora

Virus y gusanos, software maligno que dañan la computadora, un gusano se reproduce y limita la capacidad que tenemos al máximo, entonces la hace lenta, las redes también las saturan. Los troyanos se hacen pasar como un software legitimo, pero en realidad se trata de un programa que está sacando información de la computadora y que nos está exponiendo a que un hacker tome el control y pueda saquear la cuenta de banco, o saber cuál es la dirección de casa, o de cuál es el comportamiento del usuario en Internet, saber también desde donde se está accediendo Internet y saber así si la persona está o no dentro de la casa; los riesgos de la computadora pasan de nuevo al mundo físico.

El *spyware* es justamente un *software* que monitorea el comportamiento para hacer ataques enfocados a esa rutina pues es más fácil que piquen un anzuelo de spam con esos temas que más interesan.

Principales riesgos a los niños

El riesgo a los niños, son los abusos de los *Cyberbullies*, tanto los niños como los adultos se pueden ver acosados al usar Internet; esto es crítico

y es algo que está ocurriendo mucho hoy en día, por ejemplo los niños amenazados por sus compañeritos de cosas que tal vez saben que los niños hicieron entonces los extorsionan, eso es lo *cyberbullies*.

El tema de los archivos compartidos la gente lo que más busca son letras de canciones, descargar canciones, descargar videos, se abusa de archivos compartidos porque sale gratis, pero en realidad todas estas descargas gratuitas lo que traen es código malicioso que está exponiendo nuevamente a todos los ataques que vimos antes.

Contenido inquietante es todo el tema de pornografía, de violencia, es todo el tema de información que típicamente aparece en lo que se llama un *pop - ups* hoy día los niños están expuestos a todo este tipo de contenido inquietante. Si un niño explora sin ser supervisado, puede toparse con imágenes o información a la cual no debe ser expuesto.

Depredadores, ya ahí estamos hablando de lo que son depredadores sexuales, que aunque parezca mentira, de cada diez niños que navegan en Internet uno se ha topado con este tipo de depredadores, que es un número altísimo y 7 de los niños han logrado ver contenidos inquietante o de alguna forma han navegado a sitios que no deberían ver. Contaba una compañera, que al chiquito de ella lo habían suspendido de la escuela porque lo encontraron viendo pornografía en la biblioteca y el niño aseguraba que él simplemente estaba buscando algo para sus tareas y le apareció eso y claro la profesora castigó al niño y lo reprendió, pero ¿por qué la computadora de la escuela no tiene las protecciones para que no entren los *pop-ups*?, pues obviamente los están exponiendo a eso. Un 75% de los niños ven contenido inquietante buscando tareas, haciendo cosas totalmente diferentes a las que puedan aparecer.

Y el tema de la invasión a la privacidad donde es muy importante la guía que nosotros le demos a los niños e igual los adultos. Los formularios que vamos a llenar en Internet, a veces descargamos algo y sin leer el contrato se acepta y es cuando empieza a llegar correo electrónico, nos empieza a llegar información, nos empieza a descargar software, si no leemos esos formularios de que es lo que vamos a descargar nos vamos a ver plagados de mensajes que van a invadir la privacidad.

Principales amenazas a la seguridad en línea

En el tema de las amenazas a la seguridad personal, está el robo de identidad: este es un crimen en que un timador obtiene información personal y acceso al dinero y crédito de quien sustrae los datos, eso es lo que ha sucedido con el fraude electrónico, en los bancos empiezan a rastrear y se dan cuenta que la cuenta en la que están haciendo todos los movimientos es una cuenta de una persona indigente que es muy difícil que haya tenido acceso a una computadora, o bien se dan cuenta de que es una señora de 85 años que definitivamente no es el *hacker* que está haciendo el vaciado de las cuentas, pero están suplantando a esas personas para hacer una serie de delitos en línea, entonces esto es sumamente complejo.

El tema de *Phising:* e-mail enviado por criminales informáticos para engañar a fin de obtener los datos de las personas; este está en boga recientemente y es algo que probablemente todos hemos sido afectados, nos ponen un anzuelo, picamos es *phising* que en inglés significa pescar, lo que hacen es engañarnos para que suministremos la información adicional para luego poder hacer la suplantación de identidad y mucho de lo que hacen ahí es atacar entidades financieras, tarjetas de crédito y atacar lo que realmente tiene dinero por detrás.

Si uno se preguntara que es más rentable ser un hacker o ser un narcotraficante ¿qué dirían? En Estados Unidos lo que es fraude electrónico anda alrededor de 100 billones de dólares al año y lo que es narcotráfico anda alrededor de 94 y lo difícil de que agarren a un *hacker* contra lo que es agarrar un narcotraficante hace que sea un negocio muy interesante. Cuantos *hackers* han agarrado son como tres o cuatro a nivel mundial y ahora están contratados, salieron de la cárcel y son espías del lado bueno porque son muy buenos *hackers,* pero nuevamente es un negocio multimillonario que a nivel legal es un procedimiento muy complejo, y ahí ponemos las dos cosas la complejidad o lo rico que es el negocio, lo fácil que es el sistema y por otro lado lo fácil que es este negocio.

El tema de los engaños es una forma muy sutil de mentir a la gente, cuántos de ustedes no han recibido un correo que les dice tenemos una organización encargada de ayudar a los niños enfermos de cáncer

entonces por favor envíenos "X" monto y resulta que para ese "X" monto lo que se puede hacer es una transferencia de cuenta de banco, entonces ahí ya tiene el número de cuenta de banco, ya tienen la información de la tarjeta de crédito y a partir de ahí siguen haciendo cobros con esta información.

Otro tipo de engaños son las famosas cadenas "si usted no envía este correo a 10 personas usted va a tener mala suerte por 3 años", entonces claro empezamos a mandar correos como locos y obviamente lo que estamos haciendo es saturando los enlaces y lo que estamos es diciéndole a los *hackers* esta es una dirección de correo válida, aquí realmente usted puede encontrar a alguien, aquí realmente usted puede pescar, ese tipo de engaños es también lo que buscan lograr de una mentira sacar verdades. Además está el spam que lo que busca es saturar todos los enlaces con correos masivos con mensajería instantánea y otras comunicaciones en línea no deseadas.

Cuatro pasos para proteger su computadora

1. Utilice un firewall: crea una barrera protectora entre su computadora y Internet.
2. Mantenga su sistema actualizado: instale todas las actualizaciones tan pronto estén disponibles. Actualizaciones automáticas proveen la mejor protección.
3. Instale y mantenga un software antivirus: ayuda a detectar y remover los virus de la computadora previo a que cause daños. Para que el software Antivirus sea efectivo debe mantenerlo actualizado.
4. Instale y mantenga un software antispyware: para que cualquier software desconocido no pueda rastrear su activad en línea ni potencialmente robar su información.

Su Integridad

1. Mantenga un comportamiento en Internet que minimice los riesgos.
2. Administre cuidadosamente su información personal.
3. Utilice tecnologías antiphishing y antispam.

El *firewall* o la pared de fuego permite filtrar la información que entra y sale de la computadora para que no sea tan vulnerable, es como ponerle un par de candados a la puerta y que de alguna forma no sea tan simple para los atacantes entrar no es una medida infalible, pero es algo que por lo menos va a retrasar o proteger de las cuestiones más comunes o de los ataques más comunes; obviamente entre más tiempo le dedique al *firewall* más protegido va a estar, no es lo mismo un candado, que una alarma de última tecnología, con el firewall es igual hay *firewall* que son muy simples y a *firewall* que son muy complejos y que van a dar muchísima protección.

La actualización del sistema, este asunto es crítico, ningún sistema está protegido de errores, todo software tiene vulnerabilidades y las actualizaciones lo que permiten es que esas puertas que están abiertas dentro del *software* se puedan ir cerrando. Quién les diga que un *software* es 100% seguro les está mintiendo, todo *software* es vulnerable porque es hecho por humanos y tiene errores, las actualizaciones lo que vienen a hacer es enmendar ese tipo de errores que son comunes y que ha ido descubriendo puertas de entrada para los atacantes, por eso es muy importante que lo mantengan actualizado.

Mucha gente tiene instalado el antivirua en la computadora desde hace tres años, eso es como ponerse una vacuna para la gripe que está vencida, no va a proteger de los virus nuevos, las cepas nuevas que me pueden infectar a mí, es igual que en la computadora día a día están apareciendo nuevos virus, nuevos mecanismos de ataque, entonces si el antivirus no está actualizado se está totalmente desprotegido, es exactamente lo mismo.

El *antispyware* es igual que el *Spyware* tiene un comportamiento que es detectable, por ejemplo empieza a tomar todos los teclados que se dan en la computadora o se se instala en los servicios que se ejecutan a penas inicia el sistema este tipo de comportamientos es lo que el *antispyware* está tratando de detectar e igual que el antivirus tiene que mantenerse actualizado.

Otras formas de proteger su computadora

- Respaldar sus archivos regularmente.
- Piense antes de hacer clic.
- Lea la declaración de privacidad de los sitios web.
- Cierre pop-ups usando la "X" roja.

Respaldar sus Archivos

- Salve a CD/DVD, USB drive, o bien otra fuente externa.
- Utilice un servicio basado en Web de respaldo.

Aquí estamos hablando de lo que es la información, a quién no le ha pasado que trabaja en documento que esta corrupto y no tiene el respaldo o la computadora no prendió ese día y simplemente se pierde toda la información, por eso es importante respaldar los datos y cerrar los pop - ups usando la "X" roja.

Piense antes de hacer Click

- No abra anexos en e-mail a menos que sean esperados o conozca su contenido.
- Solamente descargue archivos de sitios confiables.

Lea la declaración de privacidad

Entienda en que se está involucrando antes de compartir su información o descargar contenido.

Piense antes de hacer click, esta cuestión del antispam, del phising, lo que buscan es que automáticamente le demos click, que abramos el correo. No entre a las entidades financieras desde links de correos porque se puede hacer ver exactamente igual que el link verdadero, pero por detrás lleva a otro lugar, puede hacer que el sitio se vea exactamente igual al sitio de la entidad financiera, pero se está yendo a otro lugar. Siempre que vayan a entrar al banco a cambiar su información personal, o cualquier trámite, digite usted la dirección en la barra no haga click en ningún link, es muy importante eso. Solo descargue archivos de páginas confiables, a veces necesitamos algo con urgencia y en Internet está todo pero posiblemente trae algún troyano o código malicioso, igualmente leer todos los contratos de uso y de privacidad.

Utilice la “X” roja para Cerrar Pop-ups

- Siempre utilice la “X” roja en la esquina superior de una pantalla *pop up*.
- Nunca seleccione “Si”, “aceptar” o “cancel” pues podría ser un truco para instalar software en su computadora.

El tema de la “x” roja que vemos arriba en las ventanas de los diferentes programas de la computadora, también viene si o no y cancelar, pero todos esos botones (yo como programador puedo meterle hacer la tarea que yo quiera), entonces les abro una ventana de que se acaban de ganar una vacación, le doy cancelar y lo que hago es por detrás ejecutar una serie de códigos que van a descargar información, les van a meter un troyano, o a descargar un *spyware,* en la “x” roja no les pueden meter código a su programador. Siempre que cierren un pop ups, siempre que estén navegando en Internet y les aparezcan cosas que ustedes no han llamado utilicen la “x” roja es muy importante.

Hable con sus hijos de los riesgos de la red

- Hable con sus hijos sobre los riesgos en la red.
- Hable sinceramente con sus hijos sobre los riesgos en la red, incluyendo: Criminales informáticos, contenido no apropiado e invasión de la privacidad.

Enseñeles como su propio comportamiento puede reducir esos riesgos y mantenerlos seguros mientras están en línea.

Hablar con sus hijos abiertamente de muchas de estas cosas que pasan en la red, muchas de las cosas que aprovechan los *hackers* alrededor del mundo es la ingenuidad de la gente, de que nos sentimos seguros por estar en las cuatro paredes de la casa, pero en realidad estamos expuestos a un mar de peligros como si saliéramos a las calles, donde me tengo que cuidar de que no me asalten, de que no me atropellen, de que no me roben la billetera es lo mismo.

Igual yo si estoy en línea creó que puedo dar mi información, seamos meticulosos sobre a quién estamos dando nuestros datos, a donde ponemos nuestra información personal, el mundo de Internet es igual de crítico que el mundo físico y enséñeles como el mismo comportamiento de nosotros puede disminuir los riesgos.

Aquí muchas veces los chiquitos van a saber más que uno, pero también es importante que sepamos cómo están usando la computadora, de cómo se comportan ellos en línea y a la vez darles los consejos, porque en las redes sociales ponen fotografías de la casa, del barrio, de la escuela y eso es miel para los secuestradores, por eso es muy crítico saber qué es lo que están poniendo allí.

Preste atención de lo que los niños hacen en línea

- Mantenga la computadora en un lugar compartido.
- Aprenda cómo utilizan sus hijos Internet.
- Permita que sus hijos sean los maestros.
- Enséñele a los niños a confiar en sus instintos.
- Anímelos a reportar cualquier problema.

Mantenga la computadora en un lugar compartido, donde se pueda ver realmente lo que están haciendo, poner horarios como cuando al niño le dicen: lo dejó jugar hasta que anochezca, luego se viene. Bueno lo mismo es en línea, además es el mismo peligro las 24 horas porque en Costa Rica son las 9 de la mañana y en china son las 9 de la noche, pero podrá haber un atacante que esté buscando que hacer; son una serie de peligros adicionales que nosotros muchas veces no tomamos en cuenta.

Permitir que los niños sean nuevamente los maestros y que los niños confíen en su instinto, para que si ellos sienten que hay algo que no les parece muy correcto, ellos puedan decirle mire me pasó esto, me sucedió esto, se lo juro entré a la biblioteca estaba buscando la tarea y salió pornografía, créanles los niños generalmente están diciendo la verdad. Y anímelos a reportar cualquier problema.

Mantenga la información personal privada

- Enseñe a los niños a validar con usted antes de compartir información en línea.
- Monitoree las actividades en línea de sus hijos.
- Enseñe a sus hijos a reportar actividades sospechosas.
- Ayúdelos a utilizar alias y direcciones de correo apropiadas.

Mantenga la información personal privada, enseñe a que validen con ustedes la información que van a poner en línea, casa, teléfono, fotos, que primero consulten si esto no va a traer ningún tipo de riesgos al ponerlo en línea, verificar con quién están compartiendo información en línea, ese tipo de cosas es muy importante.

Reportar cualquier tipo de actividades sospechosas. Alias de direcciones de correo apropiada. Otra cosa que me preocupa mucho en este asunto es que ¿Cuánto creen ustedes que dura un depredador en atacar a un niño en Internet? 45 minutos, dos días, una hora.

El otro día vi un video del PANI donde un chiquito -bueno no un chiquito sino alguien haciéndose pasar por una chiquita de 13 años- entró a un chat y cinco minutos después, ya el tipo estaba diciéndole "encienda la cámara, por favor compartirme fotos", 10 minutos después ya el tipo había encendido la cámara y estaba masturbándose frente a la niña. Sólo 10 minutos por eso les digo hay que ser sumamente cuidadoso donde están entrando, con quién están compartiendo información fueron sólo 6 minutos y la niña estaba expuesta a una situación totalmente incomoda.

Establezca reglas para usar internet

- No comparta archivos o abra anexos.
- No haga *click* en los *links* dentro del correo electrónico.
- Trate a los demás como le gusta ser tratado, nuevamente volvemos al tema del acoso en línea o del *cyberbulie*, no seamos matones en línea tampoco seamos irespetuosos y usémoslo como debería ser.
- Respete la propiedad de otros, el tema de música, el tema de videos, si nosotros fuéramos los dueños de esa propiedad intelectual no nos gustaría que nos la estén robando, igual con las tarjetas de crédito si encontramos una cuenta mal puesta no por eso vamos a ir y saquear a la persona.
- Nunca vaya solo a conocer una persona que conoció en Internet, es un riesgo. Si lo van a conocer vayan con alguien de confianza que este con ustedes y que pueda respaldarlos.

Utilice software de protección familiar

Ayuda a los padres a administrar el contenido que sus hijos ven, qué hacen y con quién y cómo se comunican en Internet. Hay software que permite controlar que juegos pueden usar los niños, en que horario, computadoras, que sitios pueden visitar, ese tipo de cosas, se puede restringir y poner reglas para proteger a toda la familia.

Cómo manejar problemas

- Contacte la policía y reporte cualquier amenaza en forma inmediata.
- Reporte incidentes al 911.

El tema de cómo manejar problemas, contacten a la policía y reporten igual los incidentes al 911 igual. El PANI tiene líneas abiertas, el poder judicial tiene líneas abiertas.

Se está construyendo día a día la jurisprudencia para este tipo de cosas, pero debemos reportar cualquier cosa que nos parezca sospechosa para poder entender hacia donde podemos aplicar leyes, y herramientas, hacia donde podemos hacer simplemente uso del sentido común.

Los gerentes de la seguridad de la información

Miguel Garro Arroyo

Lo que deben saber los altos ejecutivos sobre la protección de datos**.** Hoy en día los puntos de vista relacionados con la protección de datos varían de área en área dentro de las empresas, así mismo el control sobre la manipulación de los datos cada vez se vuelve más compleja y presenta mayores requerimientos regulatorios y legales que deben afrontar las empresas como un único frente.

Uno de los grandes retos de hoy en día, es la comunicación que debe existir entre las diferentes áreas de las organizaciones para establecer un mecanismo en común de cómo deben protegerse los datos de acuerdo con el área a la que pertenecen, apoyados y guiados claramente a través de la política de seguridad de la información, de forma tal que se facilite la gestión de la seguridad de la información y se adopte un esquema de protección por capas, para cumplir con los requisitos gubernamentales, legales y técnicos, los cuales aumentan proporcionalmente a las crecientes amenazas a la información. Todo esfuerzo orientado a la protección de datos debe ir enfocado a una correcta administración de los riesgos sobre dicha información.

Otro aspecto importante es el nivel de esfuerzo que debe manejarse en la protección de los datos de manera tal que se proporcione un fundamento sólido para tener una gestión de riesgos y una mejora de procesos eficientes y eficaces, así como una respuesta rápida ante incidentes, un tratamiento adecuado sobre los riesgos implica entre muchas cosas, ejecutar una serie de medidas apropiadas para mitigar los riesgos y reducir el posible impacto que tendrían sobre los recursos de información a un nivel aceptable para la empresa, tales como:

- Entendimiento en conjunto del perfil de la amenaza, vulnerabilidad y riesgo de la empresa.
- Entendimiento de la exposición al riesgo (en todos sus tipos) y las posibles consecuencias de la inestabilidad.
- Conciencia de las prioridades (tomando en cuenta el nivel de esfuerzo) de la gestión de riesgos con base en las posibles consecuencias.
- Suficiente mitigación de riesgos para obtener consecuencias aceptables del riesgo residual.
- Aceptación del riesgo a partir de un entendimiento de las posibles consecuencias del riesgo residual.

En resumen, lo anterior significa tomar decisiones en cuanto a si se debe o no mitigar el riesgo, cesar la actividad que genera el riesgo (en caso de haberla), si debe ser aceptado o si se debe transferir, a fin de garantizar una correcta gestión orientada a la protección de datos.

Retos gerenciales

Algunos de los retos gerenciales de hoy en día pueden ser resumidos al responderse algunas preguntas como por ejemplo: ¿Cómo hace la organización para proteger los activos de información e información confidencial?, ¿Quién tiene acceso a la información de negocio de la empresa? y ¿Dónde está ubicada toda la información sobre los negocios y los clientes de la empresa?, a través de dichas preguntas se pretende generar una retrospectiva sobre que tanto están consientes los gerentes sobre la importancia de la protección de datos, ya que en primera instancia es ahí donde radica el éxito de la operación de la seguridad de la información.

Así mismo, los gerentes deberían estarse preguntando ¿cómo hacer para proteger los activos de información confidencial que la empresa posee?, ¿quién tiene acceso a la información de negocio de la empresa? y ¿dónde está ubicada la información crítica de los clientes?, una vez que dichas preguntas sean respondidas por los gerentes, los mismos se podrán dar una idea sobre que tan enterados se encuentran sobre el norte que sigue su empresa en materia de protección de datos.

El Ponemon Institute lleva a cabo investigaciones independientes sobre la privacidad, la protección de datos y la política de seguridad de la información tanto en entes gubernamentales como en el sector privado y ha desarrollado una estadística a principios del año 2009 bajo el contexto de la protección de datos y su estimación para los próximos doce a veinticuatro meses sobre las amenazas a la información.

La violación de acceso a los datos se encuentra a la cabeza de las amenazas a la información, dando lugar así a la pérdida de privacidad y confidencialidad de los datos, asimismo se estima que el porcentaje que representan las amenazas sobre la información crezca para el año 2010 en un uno por ciento, representando un gran reto para las empresa el poder hacer frente a dicho crecimiento de ataques.

Violación de acceso a la información

Es importante entender que una vez comprometida la información de una organización, se da una ruptura de seguridad la cual de acuerdo con su nivel de impacto puede generar pérdida de confianza de los clientes, dando pie a la posibilidad de perderlos, mientras que el valor comercial de la marca decrementa tanto en términos comerciales como de credibilidad ante la no respuesta satisfactoria de un incidente, lo cual a su vez resulta en costos significativos para el negocio; el tiempo invertido en respuesta ante incidentes podría extenderse hasta por meses según el nivel de impacto al negocio, el tipo de amenaza y los recursos involucrados en su atención. En el peor de los casos una violación de acceso a la información podría, de acuerdo con la legislación presente y acuerdos a nivel de servicio (ANS), generar sanciones y penalidades que podrían ser millonarias y hasta ruinosas.

A raíz de todos estos riesgos, nace la necesidad de velar por los correctos mecanismo de protección implementados en la empresa con el afán de proteger los datos, así los gerentes deben de tener muy claro que cuando hay pérdida de seguridad, también hay pérdida de confianza de los clientes si no se sabe comunicar oportuna y claramente, ya que de no haber dicha comunicación se generarán dudas y probablemente la pérdidas de dichos clientes.

Un claro ejemplo de impacto negativo en el negocio sería, si se está hablando de una marca importante a nivel comercial de una empresa de publicidad y se descubre que existe fuga de información de sus operaciones, esto llega a los medios de comunicación, por ende se da pérdida de privacidad lo cual afecta desde el mercadeo hasta la imagen de esta empresa y se puede derrumbar junto con su reputación si no sabe gestionar el impacto al negocio. Así mismo se enfrentan ante grandes retos tanto en costos como en tiempos de respuesta, a veces lleva años subsanar el daño a la imagen comercial de una empresa de acuerdo con el nivel de impacto al negocio.

Responsabilidades gerenciales

Hoy en día todas las organizaciones obtienen y mantienen información en diferentes formas, utilizando un número cada vez mayor de tecnologías de información, estas cantidades crecientes de tecnologías de información no sólo brindan nuevas oportunidades de negocio sino que también aumentan los riesgos del negocio. Como resultado los gerentes tienen muchas más responsabilidades que antes sobre la protección de información, algunos de ellas son:

- Proveer patrocinio visible para la Seguridad de la Información e iniciativas de protección a la privacidad.
- Velar por la existencia, la conciencia y el apoyo constante a través de los procedimientos y las políticas de Seguridad de la Información.
- Procurar estar en cumplimiento con regulaciones aplicables y requerimientos legales.
- Demostrar diligencia ante la protección de datos al establecer políticas, aprobando normas de protección de los datos,

apoyando planes de capacitación y sensibilización de los empleados de la organización, entre otros.
- Comprender el impacto en el negocio de no proteger los datos.
- Garantizar que se están tomando las mejores prácticas para garantizar la protección de datos en toda la empresa.

Problemática inicial

A finales del año 2008 la compañía RSA efectúo una estadística que arrojó resultados en donde se indicaba que la mayoría de los empleados entrevistados dijeron que regularmente en el transcurso de sus labores diarias no seguían las políticas de seguridad de la información de la empresa; asimismo, muchos otros empleados indicaron que ellos ni siquiera tenían conocimiento de la existencia ya fuera de la existencia de dichas políticas o siquiera del contenido de las mismas, teniendo casi total desconocimiento de los actos permitidos y prohibidos en la empresa a nivel de seguridad de la información.

A partir del punto anterior, se desprenden lo problemas actuales de que enfrentan los gerentes de seguridad de la información en las empresas:

- Las políticas no son cumplidas por los colaboradores, esto ocurre porque:Los usuarios consideran dichas políticas incómodas de acatar. Los usuarios saben que no recibirán sanciones. Las políticas no son comunicadas a los colaboradores, tanto internos (incluyendo los distribuidos geográficamente) como externos (por servicios tercerizados, administrados u otro existente).

En el caso para el que las políticas no son cumplidas, existen dos aspectos interesantes, el primero es que los usuarios no les encuentran sentido ya que posiblemente no han recibido ninguna clase de inducción para concientizarlos en la importancia ni los riesgos de seguridad existentes sobre la información que manipulan dentro de la organización, o bien, saben que no van a recibir sanciones, en este caso hay carencias de definir bien cuáles son los roles o las funciones del colaborador ya que muchas veces las políticas obstaculizan

el trabajo del mismo o al menos así lo interpreta la persona, por eso hay carencias en términos generales.

Para el caso en que las políticas no son comunicadas, se debe muchas veces a que no existe un lugar donde publicarlas, no se cuentan con los medios físico o electrónicos para su distribución o por el contrario, en una empresa con mayor grado de madurez en el tema, se reciben las políticas y se firman como recibidas, sin embargo, no hay seguimiento de si el usuario entendió o no la política, para lo cual se puede recurrir a encuestas con cierta frecuencia, entrevistas con usuarios claves y demás métodos para garantizar la comprensión de las mismas, lo que a su vez generará mayor confianza y cumplimiento por parte de los colaboradores.

Requerimientos y expectativas

Las empresas se encuentran día con día con una serie de requerimientos y expectativas para la seguridad de la información, por lo que resulta de gran importancia el establecimiento efectivo de requerimientos de privacidad y seguridad de la información, esto si se desea gestionar de forma exitosa los mecanismos utilizados para la protección de datos a fin de soportar eficientemente los requerimientos del negocio.

Asimismo, es importante que se tenga un plan de clasificación y control de activos de información, dado que este es el primer paso para establecer controles sobre la información, los cuales serán exitosos en la medida en que la información haya sido clasificada eficazmente. Para salvaguardar la información y conservar una adecuada clasificación se pueden utilizar los grados de sigilos generalmente aceptados: público, privado y confidencial, sin embargo, la decisión de utilizar una cantidad específica y un nombre característico para cada clasificación, dependerá de las necesidades de clasificación de información de cada empresa, ya que la misma varía de sector en sector.

Es importante de conocer la tipificación de la información, el conocer donde se encuentra ubicada la misma, los gerentes de seguridad de la información deben saber dónde está ubicada la información

de la empresa, tanto a nivel físico como armarios, bibliotecas, centros de datos, entre otras ubicaciones físicas y medios similares, a nivel lógico, en las computadoras, en los teléfonos celulares, en los PDA's, como a nivel cultural, este último el más difícil de controlar ya que radica proporcionalmente en la concientización e identificación del empleado con el cuido que le brinda a la información de negocio que maneja según sus responsabilidades; son muchos los retos que enfrenta los gerentes de seguridad de la información, tomando en cuenta que requieren de mecanismos, tanto técnicos como no-técnicos para conocer en todo momento cómo, cuándo, desde que ubicación (física y lógica) y por quién es accesada, procesada, copiada, compartida, almacenada y hasta desechada la información en la empresa; igualmente el éxito de dicha gestión radica en que tan eficiente sea dicha labor, para ello los gerentes de seguridad de la información pueden recurrir tanto a herramientas de libre distribución como de ámbito comercial para llevar a cabo dichas labores, o garantizar que su equipo de colaboradores cuenta con las herramientas y conocimiento suficiente para que dicha gestión sea exitosa dentro de la organización.

Asimismo, no se debe olvidar que se debe documentar y comunicar como se debe proteger esta información, según el personal que la utiliza y la responsabilidad sobre la misma tomando en cuenta la cadena de propiedad: dueño, custodio y usuario.

El dueño es el ente de negocios que es responsable en primera instancia de la generación y manipulación de la información de negocio, el custodio es el ente encargado de brindar mecanismos tecnológicos para asegurar la correcta disponibilidad, integridad y confidencialidad de la información, y por último está el usuario, el cual es el que utiliza dicha información de acuerdo al proceso de negocio.

Algunas de las responsabilidades comúnmente atribuidas a los gerentes de tecnologías de la información o gerentes de TI son:

- Identificar riesgos de seguridad y privacidad.
- Identificar riesgos comunes para cumplimiento de protección de datos.
- Mapear los requerimientos para el tratamiento de los riesgos.

Identificar riesgos de seguridad y privacidad

Desarrollar evaluaciones de riesgos de seguridad con una metodología que involucre herramientas, técnicas y documentación, preferiblemente en conjunto con una evaluación de impacto a la privacidad (privacy impact assessment (PIA)), para identificar el nivel y la posibilidad de existencia real de riesgo sobre la información analizada, la identificación del riesgo en los procesos de TI es fundamental para una correcta gestión sobre protección y privacidad de la información.

Identificar riesgos comunes para cumplimiento de protección de datos

Los gerentes de TI deben identificar los mecanismos técnicos que ayudarán a que la organización se encuentre en cumplimiento tanto con las políticas y lineamientos de la empresa y con las legislaciones, regulaciones, estándares o requerimientos contractuales aplicables.

Mapear los requerimientos para el tratamiento de los riesgos

Los gerentes de TI deben mapear los puntos en común de los riesgos aplicables contra los requerimientos anteriores dentro de una matriz de riesgos para facilitar su visualización, seguimiento y control para desarrollar una adecuada metodología para el tratamiento de los riesgos.

Asimismo, se deben establecer objetivos de control y controles en los sistemas y aplicaciones de la empresa orientados a:

- Registro de eventos.
- Respaldo y restauración de datos.
- Control de acceso según responsabilidades (RBA).
- Mecanismos de autenticación.
- Mecanismos de encripción.
- Restricción de tráfico (interno y externo).
- Mecanismos contra el código malicioso.
- Sistemas de detección y prevención de intrusos.
- Monitoreo, administración y actualización de las prácticas de protección de datos sobre la infraestructura de TI.

Registro de eventos

Prácticamente cualquier ley, regulación o estándar de hoy en día requiere que toda empresa cuente con registros de eventos para contar con pistas de auditoria que permitan determinar quien acceso datos sensitivos y mostrar todos los detalles respectivos, por el otro lado los mismos sirven como última línea de defensa ante un ataque o incidente de seguridad de ahí su importancia en cuanto al manejo y retención de los mismos, igualmente de acuerdo con el tipo de regulación o estándar, se solicita una cantidad específica de años de retención, que igualmente dependerán en gran medida de la legislación aplicable de cada país para determinar la viabilidad de la misma.

Respaldo y restauración de datos

Otro componente esencial en cuanto a cumplimiento de protección de datos es garantizar la disponibilidad de la información, por ende es un aspecto de misión crítica del negocio el salvaguardar de forma apropiada, periódica y eficiente la información sensible de negocio, asimismo la utilización de mecanismos de autenticación y comprobación de la misma es imprescindible ante la necesidad de recurrir a los mismos para aplicar la garantía de disponibilidad de acceso a la información.

Control de acceso según responsabilidades

Este mecanismo conocido como RBA (Rol-Based Access) es un requerimiento de cumplimiento muy utilizado y común tanto para restringir acceso a aplicaciones, archivos y recursos de red donde se alberga información de negocio de forma tal que se garantice que solamente bajo la responsabilidad indicada independientemente del puesto o persona, se tiene o no acceso a la información protegida.

Mecanismos de autenticación

Los mecanismos de autenticación son requeridos en cualquier estándar, ley o regulación de la industria ya que permiten controlar la utilización de los recursos de la empresa a través de asignación de diversos tipos de mecanismos (dispositivos biométricos por ejemplo)

para ingresar credenciales a fin de ingresar a la información requerida, lo que permite no solo la rendición de cuentas, sino rastrear y determinar los accesos otorgados a los sistemas.

Mecanismos de encripción

Muchas de las regulaciones y estándares actuales requieren la utilización de mecanismos de encripción sobre la información crítica para el negocio ya que cada vez son más las violaciones de seguridad en cuanto al acceso de la misma, de ahí la importancia y el aliento de ánimo para que las empresas que quieran contar con mecanismos robustos d seguridad hagan su incursión en dichos mecanismos.

Restricción de tráfico

Hoy en día muchas empresas no restringen el tráfico desde y hacia Internet y en el caso de que se realice en cierta forma, no se aplica de forma efectiva, todo esto conlleva a una brecha de seguridad. Lo importante es contar con niveles o capas de seguridad de forma tal que se permita tener control sobre el tipo de datos que ingresan y egresan de la red de la empresa independientemente de donde se ubiquen los datos, ya sea en un servidor, equipo de telecomunicaciones, base de datos e inclusive las computadoras de los colaboradores, ya que esta última es la más difícil de controlar.

Mecanismos contra el código malicioso

En el mercado se encuentran muchos sabores tanto de *software* como de *hardware* para protegerse de código malicioso (*spyware, adware, troyanos,* entre otros), ya que la mayoría de estas amenazas atentan contra la seguridad de acceso a los datos, por ende es necesario que toda empresa cuente con este tipo de protección para asegurar que la infraestructura tecnológica es capaz de contener dichos riesgos a la información.

Sistemas de detección y prevención de intrusos

Los sistemas de detección y prevención de intrusos ayudan a proteger de forma efectiva la información tanto a nivel de red como a nivel

de servidores y estaciones de trabajo, permiten controlar el tráfico, prevén ataques desconocidos (ataques de día cero) y detienen ataques conocidos, igualmente deben ser personalizados de acuerdo con un estudio o análisis de riesgo anterior para garantizar cumplimiento con la documentación de seguridad de la empresa.

Gestión de las prácticas de protección de datos sobre la infraestructura de TI

Implica las buenas prácticas en cuanto a permitir y denegar acceso a la información de acuerdo con roles y responsabilidades, crear y promover procedimientos de seguridad para la gestión de la plataforma tecnológica, documentación de todos los proyectos y operaciones del áreas de TI y ¡nunca mezclar datos de desarrollo y producción!

Capítulo 9

Protección de datos

Guardianes de la información

Jorge Castro Zeledón

En Hewlett-Packard Costa Rica, uno de los negocios que manejamos es el de atención de solicitudes de seguridad. Esta tarea nos convierte en los guardianes de uno de los activos más importantes, por no decir el más importante de todos, que maneja toda empresa, el cual es la información que está almacenada en diferentes servidores.

Como parte del servicio, y para que los agentes de servicio al cliente de HP puedan dar una mejor atención a nuestros clientes, se nos da a todos un adiestramiento que no sólo cubre la parte técnica del proceso, sino que también involucra poco políticas y conceptos sobre lo que es la protección y privacidad de los datos.

El objetivo de este curso es que los agentes se sensibilicen con respecto al concepto de privacidad de los datos y que se comprometan a custodiar la información de la gente, que sepan que hay alguna información que es de carácter público y otra que no lo es. Esto hace que ellos entiendan el valor de lo que custodian y pongan mucha atención en ejecutar bien sus tareas.

Esta sensibilización es muy importante porque, desgraciadamente, en Costa Rica no manejamos el concepto de lo que es seguridad de

la información. Más bien, la tendencia del mercado y del comercio es buscar que la gente brinde toda su información a diversas empresas, por medio de mecanismos muy sencillos como encuestas o rifas. Si prestan atención a muchas de estas encuestas y rifas, una gran cantidad le piden a la persona que suministre su nombre, dirección, número de cédula, su teléfono de casa y celular, y correo electrónico, datos que son suficientes para abrir una cuenta de un banco que se podría utilizar para el lavado de dinero mediante la suplantación de identidad, pero la gente no está consciente de este riesgo.

Pero ese no es el único problema. Esos datos después son descartados, se desechan, se comparten con otras empresas, se procesan de alguna manera para determinar un perfil socioeconómico de la persona. Los datos pueden tomar múltiples rumbos. Una vez que los damos no sabemos realmente qué pasa con ellos, y muchas de estas empresas que recopilan nuestra información no tienen políticas del manejo de datos claras que nos indiquen qué sucede con la información, cómo se custodia o cómo se destruye.

Hoy en día hay muchas empresas que se dedican a recolectar esos datos y que con sólo ingresar nombre y apellidos dan una gran cantidad de datos relacionados con nosotros. Esta información nos dice claramente dónde trabaja, que propiedades tiene, cuál es el salario, y otros datos de la persona consultada. Esta es demasiada información que no sabemos cómo se está utilizando y que puede ser utilizada contra la ciudadanía de diversas maneras. La suplantación de identidad es una posibilidad, así como lo es el fraude, las estafas e incluso el determinar a qué persona es rentable secuestrar.

Recientemente tuve una experiencia relacionada con este tema con una empresa que trae paquetes que compro por Internet. Este es un servicio muy común, que simplemente consiste en la recepción de un paquete en una dirección en Miami, y la empresa lo transporta a Costa Rica, y hace todos los trámites aduanales pertinentes. Un día una de estas compañías me solicitó una serie de datos que yo considero que no tienen ninguna relevancia con el servicio que me estaban brindando. Entre estos datos, ellos estaban preguntando si tengo casa propia o alquilada, cuantos carros tengo, si tengo una

lavadora, cocina eléctrica o de gas, lo cual nada tiene que ver con el negocio que esa compañía tiene conmigo.

Estas preguntas hacen pensar dos cosas: que la empresa está tratando de definir mi perfil socioeconómico para enviarme algún tipo de propaganda especializada según mi nivel de ingreso, o bien que la compañía puede estar recolectando esos datos para vendérselos a un tercero.

Actualmente, la legislación solo cubre algunas empresas de sectores específicos, como lo es el sector financiero. Fuera de este, no tenemos legislación, y por ende se pueden usar los datos de la manera que la empresa crea conveniente, pueden estarse dando para usos de mercadeo o para usos dañinos, no sabemos si un tercero está vendiendo esos datos para determinar a quienes potencialmente se podría asaltar o robar.

Otro asunto importante es que a nivel de gobierno se sigue hablando del tema de reducir la brecha digital, en alfabetizar digitalmente. Estas son iniciativas que eventualmente pueden ayudar al desarrollo del país, pero estas no se están ejecutando de la mano de una educación adecuada sobre la seguridad de la información. Cada vez estamos conectando más gente a Internet, que está dispuesta a publicar su información privada en redes sociales, que está dispuesta a hablar con desconocidos en Internet, a brindar su información en cuanta encuesta hay o por correo electrónico con la promesa de ganar un teléfono celular, ignorantes del riesgo que implica y sin aceptar dicho riesgo explícitamente.

Entonces surge la pregunta, ¿si seguimos por este rumbo, a dónde va a llegar nuestra información? Incluso la información puede estar saliendo fuera de nuestras fronteras.

Por todo lo anterior, es importante que como nación empecemos a trabajar en darle herramientas culturales a la gente, en concientizar sobre cuál es la importancia de los datos que maneja una persona, o bien una empresa.

También hay que normar la seguridad que tienen los repositorios de información de las empresas que se dedican a consolidar los datos de la gente. En uno de mis cursos de seguridad de aplicaciones, uno de

los estudiantes ya conocía la manera de entrar a uno de estos sitios sin necesidad de un usuario o una contraseña específica. El pudo ingresar y consultar la información de la persona que a él se le ocurriera en el momento, utilizando técnicas de *hackeo* simples. No hay una sola política o ley que le exija a estas empresas una serie de controles mínimos que deberían tener para el manejo de los datos, eso significa que ya en este momento hay terceros con acceso a esa información y posiblemente las empresas no se dan cuenta de la fuga de esta información. Si no se toman las previsiones del caso podríamos caer en una situación en la cual todos los datos quedan a la deriva.

El mensaje que todos deberíamos retener en nuestras mentes para luego divulgar es que no solo hay que implementar los controles técnicos adecuados sobre la información, sino que se debe definir un estándar de cuál es el nivel mínimo de seguridad que debería tener la información de toda la población y definir además cual es esa información que se debe resguardar. En paralelo, como sociedad debemos hacer conciencia del valor de nuestra información, así como muchas empresas lo han hecho ya.

Modelo para la Seguridad de la Información

Álvaro G. Jaikel Chacón

La seguridad de los datos se ha vuelto un imperativo en muchas organizaciones, de la que cada vez más y más instituciones adquieren conciencia de la problemática, e implementan medidas de complejidad, profundidad y amplitud creciente, para gestionar los riesgos asociados.

La seguridad de la información contiene cuatro principios básicos para su adecuada protección:

1. Confidencialidad: sólo quienes estén expresamente autori zados, y necesariamente lo requieran, deben tener acceso a esta información.
2. Integridad: únicamente quienes estén expresamente autoriza--dos y cuenten con ese mandato formal, pueden modificar datos. Si los datos son definitivos, no deben ser modificados.
3. Disponibilidad: la información debe estar disponible cuándo, dónde, cómo, y por quién se requiera, siempre y cuando se cumplan los requerimientos establecidos.
4. Autentificación: es el procedimiento donde se comprueba y verifica fehacientemente que quién acceda a la información, está expresamente autorizado y es quien dice ser.

Los principales retos a los que enfrentan las organizaciones en seguridad de la información, son coincidentes para muchos investigadores y especialistas, quienes en términos generales los agrupan en las cuatro caracterizaciones siguientes.

Economía globalizada

La apertura de mercados y el creciente movimiento de desregulación e internacionalización de muchas de las economías del planeta, ha incrementado exponencialmente las transacciones, muchas de las cuales contienen información de carácter confidencial, que debe ser administrada por las partes para garantizar el buen uso de los datos.

Riesgos empresariales cambiantes

La dinámica de negocios ha venido adecuándose y modificándose cada vez con mayor celeridad en prácticamente todas las organizaciones. Los constantes cambios en el entorno generan adaptaciones en el interno que conducen a una continua aparición, variación y desaparición de retos asociados con la seguridad de la información.

Colaboración cruzada inter e intraorganizacional

La introducción en las cadenas de valor de las organizaciones, de proveedores y clientes que interactúan directamente con estas; la necesidad de establecer, operar y mantener alianzas estratégicas; entre otras muchas razones, ha incidido en una enorme apertura en el trasiego de datos dentro de las mismas organizaciones y cada vez más entre ellas, lo que amplía el espectro de los riesgos que deben ser gestionados para mantener una seguridad aceptable de la información.

Comercio en línea

La oportunidad de establecer relaciones comerciales en todo el mundo, en el horario que los clientes prefieran, y con el cierre automático de pedidos de bienes y servicios, y en algunos casos su entrega inmediata; someten a las organizaciones que utilizan estas tecnologías, tanto a los innumerables beneficios que conceden, así como a las amenazas constantes, diversas y permanentes para vulnerar la seguridad de la información transaccional, así como los equipos y aplicativos que permiten su ejecución.

Estos retos deben ser atendidos con una visión más preventiva que curativa, dado que ya se ha demostrado en muchas instancias, el beneficio económico que involucra la previsión ante la materialización de un riesgo de seguridad de la información en particular. Las principales corrientes para enfrentar estos retos pueden resumirse en las cuatro, que se indican a continuación.

- **Investigación dirigida**
  Mucha investigación se desarrolla para identificar anticipa damente, cuáles pueden ser las amenazas para la seguri dad de la información, que implican entre otras, las tenden cias tecnológicas; los cambios en las formas de hacer nego cios; y las vulnerabilidad emergentes en el uso y aplicación de las plataformas más comunes en el mercado.

- **Establecimiento de estándares**
  Constituyen recopilaciones estructuradas de mejores prác ticas actualizadas periódicamente. Ejemplos de estos relacionados con la seguridad de la información son la familia ISO 27000; el Marco de referencia Enterprise Risk Management, ERM, emitido por el Comité de Organizaciones Patrocinadoras, mejor conocido como COSO; o el marco de referencia CobiT emitido por el Instituto de Gobierno de la Tecnología de Información, de la ISACA.

- **Desarrollo de herramientas**
  Gran cantidad de desarrolladores privados, así como pro veedores de tecnología en general, están constantemente liberando herramientas que permiten mayor control de las vulnerabilidades que se van produciendo y descubriendo con el uso de nuevas tecnologías. Las nuevas vulnerabilidades identificadas, pueden ser atendidas e incorporadas rápidamente por medio de las modificaciones en las rutinas, programas, o configuraciones, también por los cambios emitidos por los proveedores de aplicaciones, denominados como “parches”.

Tecnologías emergentes

Las tecnologías emergentes, por lo general ya consideran las lecciones aprendidas que les son aplicables en el tema de seguridad de la información, e incorporan la prevención de amenazas que si bien hoy no lo constituyen, es factible que lo sean en el futuro inmediato.

El reto de la seguridad de la información, sin embargo, es visto de manera particular por las organizaciones, que manifiestan algunas de las situaciones que se describen a continuación.

Las formas de ver la seguridad de la información o visiones comentadas anteriormente, han evidenciado, entre otras, las situaciones siguientes:

La indefinición o el establecimiento poco claro de las funciones y responsabilidades relacionadas con la seguridad de la información puede producir vulnerabilidades en el manejo de la información.

El manejo de la seguridad de la información en ámbitos específicos y aislados, adicionalmente a la lenta y retardada velocidad de respuesta ante incidentes, usualmente viene acompañada de duplicaciones de gastos, entre los que posiblemente existan algunos que sean del todo innecesarios.

El establecimiento deficiente de las fronteras entre las áreas funcionales y los procesos, los que comúnmente se efectúan parcialmente en distintas áreas funcionales, conduce a menudo en una marcada dilución de la responsabilidad para el rendimiento de cuentas, en la que resulta difícil a veces, hasta el aplicar medidas sancionatorias.

El valor de la seguridad de información se manifiesta en la prevención de aquellas situaciones relacionadas que amenacen la consecución de los objetivos del negocio, y en tomar medidas de mitigación para los eventos que se requiera gestionar.

Las diferentes formas de conceptualizar y/o implementar la seguridad de la información, generan situaciones como las que citamos a continuación.

- La gran mayoría de los funcionarios de las organizaciones consideran la seguridad de información una disciplina de carácter técnico, que no tiene mayor relación con las tareas propias de las funciones que realizan, y por lo tanto no es inherente a su cargo;
- Existe una confianza advertida que al disponerse de herramientas tecnológicas, ya se está suficientemente protegido, aunque esté más que comprobado que su solo uso, no es por sí mismo la solución;
- Se requiere promulgar políticas específicas para proteger la información, apoyadas en estándares y lineamientos acordes a la naturaleza y necesidades de la empresa; que permitan y faciliten el alineamiento, desarrollo e implementación del programa institucional de seguridad de la información;
- Muchas organizaciones no tienen establecido ni en operación, la clasificación de niveles de confidencialidad de la información, lo que produce lagunas en las expectativas de cómo utilizar, compartir, trasmitir, y destruir la información;
- Aunque la cultura del entorno y la de la empresa constituyen elementos fundamentales en el éxito de la gestión en este ámbito, muy pocas veces se considera el impacto de esta en el desarrollo e implementación del ambiente de seguridad corporativa, tanto física como lógica;
- La manera en cómo la gente utiliza y reacciona ante las tecnologías de información, son determinantes al establecer la estructura y el "modus operandi" de programas que manejen eficiente y efectivamente la seguridad;
- La sostenibilidad del programa de seguridad de información en el cometido y en el tiempo, requiere entre otros elementos, de las interacciones recíprocas entre la organización, la gente, los procesos y la tecnología;
- No debe pasar desapercibido cómo el gobierno de tecnología, la cultura, el factor humano y la arquitectura, pueden facilitar u obstruir la habilidad para proteger la información gestionar los riesgos asociados;

- Los constantes cambios en el entorno de negocios y dentro de la misma empresa, le exigen un esfuerzo permanente para mantener alineado el programa de seguridad de la información con requerimientos y amenazas cada vez más demandantes.

Esta variedad de conceptualizaciones dificultan el manejo de la seguridad de la información bajo un enfoque integral, que satisfaga de forma balanceada los distintos conceptos, dentro de los que podemos observar incluso contradicciones evidentes y matices que pueden ser interpretados de distintas maneras.

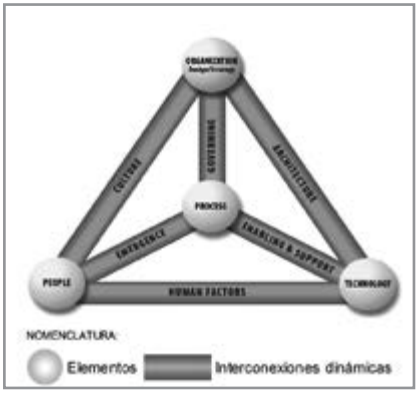
Una de las organizaciones internacionales que más se comprometió con esta búsqueda, fue ISACA, nombre genérico con el que se denomina la entidad, anteriormente conocida por su denominación en idioma inglés como Information Systems Audit and Control Association, que amplió su radio de acción para comprender e integrar las disciplinas: de gestión, control, seguridad, auditoría y gobierno de las tecnologías de información.

Al comienzo de la Investigación el Information Technology Governance Institute, ITGI, o en nuestro idioma Instituto de Gobierno de la Tecnología de Información; organización perteneciente a ISACA y encargada de la investigación y desarrollo de marcos de referencia demandados por los miembros y la comunidad internacional, inquirió entre la red mundial de asociados de ISACA, institutos de investigación, agencias especializadas y otras entidades afines, acerca de los esfuerzos que se estaban desarrollando para satisfacer los requerimientos de la comunidad respecto a la seguridad de información en las organizaciones.

Al analizar, valorar y seleccionar la información recopilada, seleccionó de una serie de opciones, los estudios que estaba llevando a cabo el Instituto para la Infraestructura de la Información, de la Escuela de Negocios de la Universidad de Southern California.

ISACA firmó un convenio con dicha organización para continuar las investigaciones desarrollar el Modelo al que hacemos referencia en este documento. El convenio formal fue suscrito en el año 2008.

Figura No. 1
Representación visual del Modelo de Negocio de Seguridad de Información



Producto del convenio y del avance de la investigación, a mediados de 2009 el ITGI publicó el documento denominado "An Introduction to the Business Model for Information Security", traducido al idioma castellano como: "Una Introducción al Modelo de Negocio para Seguridad de Información".

El Modelo de Negocio para Seguridad de Información de ISACA-ITGI mantiene la orientación al negocio para la gestión de la seguridad de información, así como los conceptos originales con el que fue diseñado, incluyendo el pensamiento sistémico, utilizado para aclarar interrelaciones empresariales complejas que permitan lograr mayor efectividad en la seguridad de información.

Presenta un enfoque dinámico, predictivo, flexible y holístico que resuelve en buena medida, las principales dificultades identificados por los técnicos y profesionales informáticos, así como las planteados por directivos y administradores de muy diversas organizaciones alrededor del mundo, cuyas opiniones y requerimientos fueron considerados para llevar a cabo esta iniciativa.

En la Figura No. 1 presentamos una ilustración del modelo, visualizado como una figura flexible y piramidal enmarcada en tres dimensiones, y constituida por cuatro elementos relacionados por seis interconexiones de carácter dinámico, en la que todos los componentes interactúan con cada uno de los demás. Si una parte del modelo se cambia, omite o maneja inapropiadamente, el equilibro del modelo se pone en riesgo. Las interconexiones dinámicas ejercen también como una especie de tensores, que ejercen en él efectos semejantes a fuerzas de compresión y expansión como respuesta a los cambios experimentados, que permiten al modelo la adaptación necesaria a nuevas circunstancias.

La conceptualización de los cuatro elementos que constituyen el modelo se resume en los párrafos siguientes.

1. Estrategia y diseño de la organización

La organización se conceptúa como un conjunto de personas, activos y procesos que interactúan unos con otros, con funciones definidas, que trabajan para el logro de una meta común. La estrategia de la empresa especifica las metas y objetivos a alcanzar por el negocio, así como los valores y la misión de este. Es la "formula" para el éxito del negocio y establece el rumbo, que debe ser adaptado a los cambios en los factores internos y externos. Los recursos son los puntos de partida para el diseño de la estrategia, dentro de los que se encuentran entre otros: las personas, equipos, y conocimiento. El diseño define el cómo la organización desea implementar su estrategia, y está fuertemente determinado, entre otros, por los procesos, la cultura y la arquitectura del negocio.

2. La gente

Dentro del elemento gente o personas, no solo se considera el recurso humano, incluyendo además los aspectos de seguridad que le son inherentes. Define, -a través de diseño- quién implementa cada componente de la estrategia. Dado representa una colectividad humana, deben tomarse en consideración los valores, comportamientos y sesgos organizacionales. A nivel interno, es crítico para la Oficialía de Seguridad, el trabajo conjunto con los departamentos Legal y de Recursos Humanos, para establecer aspectos como: estrategias de reclutamiento, asignaciones a los empleados, y terminación de contratos, entre otros.

3. Los procesos

Los procesos incluyen los mecanismos formales e informales de diverso carácter y complejidad, establecidos para que las actividades se realicen, y proporcionan un nexo vital con las interconexiones dinámicas. Los procesos identifican; miden; gestionan y controlan los riesgos, la disponibilidad, la integridad y la confidencialidad; así como también el rendimiento de cuentas. Parten de la estrategia y permiten implementarla en las unidades organizacionales. Para

generar ventajas a la organización, los procesos deben: a- satisfacer los requerimientos del negocio y estar alineados con las políticas, b- Considerar situaciones de emergencia y adaptarse fácilmente a los cambios, c Estar documentados y actualizados, así como comunicados a los involucrados, d- Revisarse periódicamente para asegurar que mantienen la eficiencia y efectividad.

4. Tecnología

El elemento tecnología está compuesto por todas las herramientas, aplicaciones e infraestructura que permiten hacer más eficientes los procesos. Como un elemento evolutivo que experimenta constantes cambios, posee sus propios riesgos dinámicos. Dada la dependencia tecnológica de las empresas, la tecnología constituye una parte fundamental de la estructura y los componentes críticos para el logro de su misión. Como ya comentamos, a menudo la tecnología es vista por la administración como el medio para resolver las amenazas y riesgos de la seguridad de información. Aunque los controles tecnológicos son valiosos para mitigar algunas clases de riesgos, la tecnología "per se" no debería verse como la solución para la seguridad de información. La tecnología es impactada fuertemente por los usuarios y por la cultura organizacional. Algunas personas no confían en la tecnología, algunos aún no han aprendido a utilizarla, mientras que otros sienten que les hace innecesariamente lenta sus labores. No importan las razones, los responsables de la seguridad de información deben permanecer siempre alertas pues muchas personas intentarán obviar los controles informáticos.

Las interconexiones dinámicas son las que vinculan los elementos del modelo y ejercen fuerzas multilaterales que se expanden o comprimen con los cambios que experimentan. Las acciones y comportamientos que ocurren en las interconexiones dinámicas pueden tanto sacar de balance el modelo, o volverlo al equilibrio. Las descripciones generales de las seis interconexiones dinámicas se resumen a continuación.

Gobierno

El gobierno empresarial fija el rumbo y la dirección de esta, y requiere liderazgo estratégico. Establece los límites dentro de los

cuales opera la empresa, y se implementa con procesos para medir el desempeño, describir actividades, y lograr el cumplimiento normativo; todo mientras proporciona adaptabilidad ante condiciones emergentes. El gobierno incorpora el aseguramiento que los objetivos estén determinados y definidos; la confirmación que los riesgos se gestionan apropiadamente y la comprobación que los recursos se utilizan responsablemente.

Cultura

La cultura es el patrón de comportamientos, creencias, supuestos, actitudes y formas de hacer las cosas. Es emergente y aprendido, y origina una sensación de confort. La cultura evoluciona como una especie de historia compartida conforme un grupo pasa un conjunto de experiencias comunes. Estas experiencias similares producen ciertas respuestas, que se convierten en comportamientos compartidos y esperados. Estos comportamientos llegan a ser reglas no escritas, que se convierten en normas aceptadas por las personas que tienen esa historia compartida. Es importante comprender la cultura de la organización porque influencia profundamente cuál información es tomada en cuenta, cómo se interpreta, qué se va a hacer con esta. La cultura se crea por factores internos y externos, y es influenciada, así como influencia los patrones organizacionales.

Habilitación y apoyo

Este interconector relaciona los elementos tecnología y procesos. En primera instancia para apoyar en la verificación que las personas cumplen con las medidas de seguridad tecnológica, políticas y procedimientos que facilitan los procesos. La transparencia puede generar aceptación para los controles, si permiten que los usuarios no se vean afectados por estos en su desempeño efectivo. Muchas de las acciones que afectan tanto la tecnología como los procesos ocurren en esta interconexión. Las políticas, estándares y lineamientos deben diseñarse para apoyar las necesidades del negocio al reducir o eliminar los conflictos de interés, mantener la flexibilidad para adecuarse a los cambios de objetivos de negocio, y ser aceptables y fáciles de seguir para las personas.

Surgimiento

El término Surgimiento posee la connotación también como: aparición, desarrollo, crecimiento y emerger; y se refiere al patrón que surge en la vida de la organización sin que tenga una causa aparente, y cuyos resultados son imposibles de predecir ni controlar. Esta interconexión dinámica entre gente y procesos es el punto para introducir posibles soluciones como ciclos de retroalimentación; alineamientos con la mejora de procesos, consideración de situaciones emergentes en el ciclo de vida de sistemas, control de cambios y gestión de riesgos.

Factores humanos

Esta interconexión representa la interacción y la brecha entre la tecnología y la gente, y como tal es crítica para el programa de seguridad de información. Si las personas no comprenden cómo utilizar la tecnología, no la adoptan o no siguen las políticas pertinentes, pueden surgir serios problemas de seguridad. Problemas internos como la filtración, robo o uso indebido de datos pueden ocurrir dentro de esta interconexión. Pueden aparecer factores humanos de edad, nivel de experiencia y/o experiencias culturales. Dado que los factores humanos son componentes críticos en el mantenimiento del balance dentro del Modelo, resulta importante capacitar a todo el personal en las habilidades requeridas.

Arquitectura

La arquitectura de seguridad es la encapsulación comprensiva y formal de los procesos, gente, políticas y tecnología que contiene las prácticas de seguridad de la organización. Una arquitectura de información robusta, resulta esencial para comprender las necesidades de seguridad del negocio, y el consecuente diseño de seguridad de esa arquitectura. Es dentro de esta interconexión dinámica que la organización puede ejercer su protección con mayor profundidad. El diseño describe cómo se ubican los controles de seguridad y cómo se relacionan con toda la arquitectura de la tecnología de información. La arquitectura de seguridad de la empresa facilita la seguridad en las líneas de negocio de una forma consistente y costo

efectiva, que le permite ser proactiva en las decisiones de inversión en seguridad.

Uso del modelo y beneficios derivados

Debido a la celeridad con que se desarrollan actualmente los negocios y transacciones derivadas, las empresas requieren comprender lo que está sucediendo, en tiempo real, y ser capaces de diseñar soluciones rápida y efectivamente. Al aplicar los conceptos del pensamiento sistémico, el modelo permite un enfoque de ciclo de gestión de seguridad en la empresa. El modelo está orientado fundamentalmente a la seguridad, sin embargo, una vez que está completamente adoptado, puede impactar positivamente también otros procesos funcionales.

El modelo ofrece beneficios para una gama de los sujetos relacionados con la organización, al reducir costos, mejorar el desempeño, fomentar un mejor entendimiento de los riesgos de la empresa, incrementar el trabajo de equipo y reducir la duplicación de esfuerzos.

El buen uso del modelo prepara a la empresa para enfrentarse a situaciones actuales y futuras como: a) requerimientos normativos, b) globalización, c) crecimiento y escalabilidad, d) sinergias organizacionales, e) evolución tecnológica, f) economía de mercados, g) recursos humanos, h) competencia, i) amenazas cambiantes, e j) innovación, entre otras.

El empleo de este modelo ayudará a los administradores a aprender cómo manejar la agregación de riesgos producidos por la combinación e interrelación de eventos y dimensiones dinámicas; más que por la vía de causa efecto. Como resultado, pueden utilizar el modelo para crear herramientas que ayuden a las personas a definir procesos sistemáticos para mejorar la gestión de riesgos en la organización.

Información adicional acerca de ISACA, el Instituto de Gobierno de Tecnología de Información, o del Modelo, puede obtenerse en la dirección electrónica de ISACA Internacional www.isaca.org

NIC-Internet Costa Rica

Jéssica Calvo Delgado

Con el fin de introducirlos y tener un conocimiento más amplio, Internet está basado en el Sistema de Nombre de Dominio. Están los dominios genéricos que son por ejemplo los .com y .net, también están los .org. Estos no están otorgados a ningún país en especifico, son delegados a empresas a nivel mundial para su administración.

Por otro lado existen los dominios código país, que es el dominio que se le asigna a cada país. En el caso de Costa Rica es .cr, para Gran Bretaña es .uk.

La Academia Nacional de Ciencias comenzó la administración del .cr a inicios de los 90. Realiza esta gestión a través de su unidad NIC-Internet Costa Rica, la cual se encarga de la operación del Domino Superior .cr.

Este servicio de registro de nombres de dominio que se presta a nivel local y mundial, porque cualquier persona puede registrar un dominio bajo el dominio .cr, se hace a través del portal www.nic.cr. Este contiene información general sobre el servicio, y además, es el medio a través del cuál los usuarios pueden hacer cualquier tipo de transacción sobre su dominio.

Información que administramos

- Datos de los contactos de un nombre de dominio.
- Datos de un nombre de dominio:
  Nombre de dominio
  Titular
  Contactos
  Servidores de nombre, direcciones IP
  Fecha vencimiento
- Gestiones de un nombre dominio (pagos, modificaciones, otros).
- Información administrativa.

¿Qué tipo de información administramos?

Administramos información de los contactos de los dominios que son personas físicas. Administramos información del dominio, como el nombre del dominio, titular, los contactos, información técnica (servidores de nombre, direcciones IP), entre otros. Administramos también todas las gestiones relacionadas con los nombre de dominio.

Todo registro de dominio y toda transacción sobre un dominio genera una serie de transacciones adicionales que administramos de manera electrónica. Además, administramos información de tipo administrativa que no deja de ser menos importante que la información de los usuarios, que la información propiamente de y de los dominios.

¿Cómo administramos nosotros esta información? ¿Cuál es la infraestructura crítica?

Una parte muy importante es la base de datos del sitio web www.nic.cr, la cual consideramos parte de nuestra infraestructura crítica. Esta es la base de datos donde está almacenada la información de los dominio (contactos, datos sobre los dominios). Otra parte de la información está en el servidor primario de nombres ns.cr, donde están registrados los nombres de dominio con sus servidores de nombre y direcciones IP. Este es él que se anuncia en Internet, y el que permite que los sitios web bajo .cr sean visibles, por esto es parte de nuestra infraestructura crítica.

Después está el servidor de correo. Todas las transacciones que recibimos de los usuarios a través del sitio web www.nic.cr generan un correo a los contactos del dominio. Las transacciones se gestionan por medio de un sitio privado y se generan correos electrónicos automáticos a los contactos del dominio. Es por esto que es importante que cada dominio tenga los dos contactos, y es por esto que también el servidor de correo es crítico en nuestra organización.

Políticas de seguridad

Políticas para el funcionamiento del Dominio de Nivel Superior .cr

Sobre privacidad:

- Información suministrada por el usuario vía http://www.nic.cr es protegida por un certificado de seguridad basado en el protocolo SSL, emitido por una entidad certificadora reconocida.
- No se almacenan datos completos de tarjetas.
- El envío de información a los usuarios está protegida por un *Digital IDs for Secure Emai*l de una entidad certificadora reconocida.
- Cierta información suministrada por el usuario es pública por medio de la consulta WHOIS.

Toda la información que es suministrada por los usuarios a través de la parte transaccional del sitio web www.nic.cr está protegida por el protocolo de seguridad SSL, al contar el sitio web con un certificado de seguridad basado en este protocolo. Todos los nombres de dominio tienen un costo, entonces una de las políticas es no almacenar el número completo de la tarjeta sino solo algunos dígitos para gestiones que haya que atender. El correo electrónico cuenta con un *Digital IDs for Secure Email* que básicamente le dice al usuario que quien envió la comunicación es *NIC-Internet Costa Rica* y que la información no fue leída durante su envío.

Otra política que tenemos es hacer pública, a través de una consulta que se llama *Whois*, cierta información que el usuario nos suministra en el proceso de registro. Es información del dominio. En

general ustedes pueden ver que para un dominio genérico o dominio código país, existe una herramienta que se llama *Whois*, la cual muestra información del dominio por si pudiera surgir la necesidad de contactar a alguien del dominio.

En nuestras políticas de seguridad o de privacidad le indicamos a los usuarios los medios seguros que se utilizan para capturar la información, cual información no se suministra al público, y cual información va a estar disponible a través de *Whois*.

Base de datos web

- Protegida por niveles de seguridad implementados por el proveedor de infraestructura (*hardware/software-firewalls*-, acceso físico restringido, procedimientos).
- Niveles de seguridad adicionales de NIC-Costa Rica: accesos remotos seguros por https, SSH y accesos restringidos por IP de origen.
- Cambios periódicos de claves.
- Manejo de bitácoras.
- Cambios a base de datos y aplicación web primero en ambiente de pruebas, luego en producción.
- Respaldos automáticos diarios y semanales a base de datos y sitio web. Se almacenan en lugares distintos.

La base de datos está hospedada en un Data Center, tiene los primeros niveles de seguridad de éste a nivel de *firewall, hardware, software* y acceso restringido al servidor donde está la información. Además de estas condiciones de seguridad que da el proveedor, tenemos nuestras políticas relacionadas con accesos restringidos y accesos seguros cuando necesitamos ingresar a la base de datos. Se trabaja con cambios periódicos de claves. Las bitácoras son fundamentales cuando usted necesita ampliar la información, cuando necesita reconstruirle algún evento al usuario.

Una política de seguridad importante es que no se hacen cambios en el sitio web en producción o lo que se llama en caliente, sino que se hacen en ambientes de prueba, y luego se pasan a producción.

Los respaldos son críticos, principalmente para reconstruir escenarios, que nos hemos visto en la necesidad de hacer. Importante también es el almacenamiento de respaldos en diferentes lugares físicos para no concentrar el riesgo.

Servidor primario de nombres ns.cr

- Protegido por medidas de seguridad del Centro de Informática de la Universidad de CR (restricción de puertos TCP de entrada y salida, *firewall*, control de acceso físico).
- Niveles de seguridad adicionales de NIC-Costa Rica (implementación segura del sistema operativo, solo se habilitan los accesos indispensables para operar).
- Respaldos automáticos diarios de tablas DNS y configuración. Se almacenan físicamente en lugares distintos.
- Cambios deben ser comunicados a grupo técnico, y contar con autorización.
- Cambios periódicos de claves.

El servidor primario de nombres ns.cr, es el que anuncia todos los dominios .cr en Internet. Está ubicado aquí en la Universidad de Costa Rica, en el Centro de Informática. Está protegido por las medidas de seguridad de la universidad, siendo éste el primer nivel de seguridad. Tiene las restricciones de puertos de la universidad, con excepciones a solicitud nuestra como operadores de este servidor.

También generamos al igual que se hace con la base de datos, respaldos. Generamos respaldos de las tablas (datos) y de las configuraciones. Con el servidor primario nunca hemos tenido que hacer uso de estos respaldos.

Algo importante en la administración del servidor primario es que es muy restringido el acceso para los registros en el mismo. Son muy pocas las personas quienes tienen acceso. Los cambios en configuraciones son muy restringidos, y tienen que ser comunicados al equipo técnico para ver si se procede o no con el cambio, se necesita de aprobación.

Al igual que con la base de datos, se realizan cambios periódicos de claves.

Servidor de correo

- Antivirus.
- Antispam.
- Diferentes listas negras de *spam*.
- Solo protocolos seguros para mandar y recibir correo.
- Respaldos periódicos de configuración y buzones.
- Cambios periódicos de claves.

Después está el servidor de correo, que como les comentaba también es parte de nuestra infraestructura critica. Lo protegemos con políticas antispam, antivirus, cambios periódicos de clave, respaldos automáticos en configuraciones y buzones, etc. Se usan solamente protocolos seguros para el envío de correo.

DNSSEC

DNSSEC es la extensión de seguridad del protocolo de DNS."Al mirar el tema general de la confianza e Internet, una de las partes más críticas de la infraestructura de Internet que parece ser un punto de ancla central de confianza es el Servicio de Nombres de Dominio, o DNS.…La habilidad para corromper el funcionamiento del DNS es una de las maneras más efectivas de corromper la integridad de las aplicaciones y servicios basados en Internet." Geoff Huston, agosto 2006, *Internet Society*.

Básicamente hasta acá he hecho una descripción de cómo manejamos los datos que nos brindan los clientes en el registro de los nombres de dominio y para la operación de los dominios, al igual que la información que nosotros mismos generamos producto de esta administración.

Hay un proyecto de gran relevancia que empezamos a trabajar el año pasado (2008). Tiene que ver con la cita de Geoff Huston uno de los colaboradores de la *Internet Society*, ente encargado de emitir los estándares bajo los que se desarrolla la estructura de Internet y se continúa desarrollando, lo comentado fue: una de las partes más críticas en el desarrollo de Internet o el punto ancla para la confianza en esta Red es el Sistema de Nombres de Dominio (DNS) y la confianza que se tiene en éste. Entonces: "La habilidad para corromper el funcionamiento del DNS es una de las maneras más

efectivas de corromper la integridad de las aplicaciones y servicios basados en Internet."

Simplemente lo que está diciendo es que aquello que pueda socavar la confianza en el Sistema de Nombres de Dominio tiene un impacto muy importante en la integridad de Internet y los sistemas basados en esta Red.

Hay una vulnerabilidad identificada por Dan Kaminsky en el año 2008, que tomó gran importancia y se le conoce como el *Efecto Kaminsky*. Consiste en que cuando un atacante puede introducir en un servidor recursivo direcciones IP erróneas para un nombre de dominio, cuando alguien digita en un buscador el nombre de dominio al que necesita llegar, pero a éste nombre le han cambiado la dirección IP en el servidor recursivo, la persona va a ser direccionada a una página falsa, a una página errónea.

Que significa esto? Que los que quieren delinquir pueden hacerlo dirigiendo a las personas a una página errónea, controlando el tráfico a través de ésta técnica llamada envenenamiento del caché. Así, si se desea ir a www.nación.com y el servidor recursivo no tiene la dirección correcta para este nombre sino una dirección modificada, puede redirigir al usuario a una página web que no es la verdadera. Con esta técnica se pueden cometer actividades delictivas obteniendo información privada del usuario.

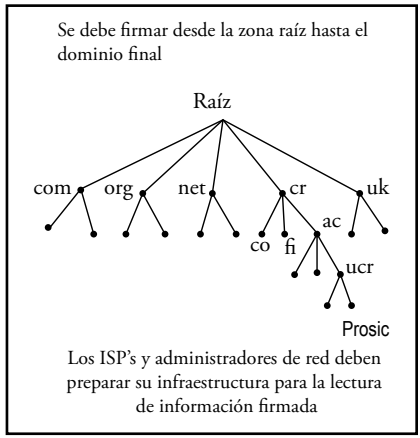
Características DNSSEC

- Es una especificación de seguridad del protocolo DNS.
- Diseño lidia contra ataques de envenenamiento del cache.
- Su objetivo es validar la autenticidad e integridad de las respuestas de DNS.
- No cifra los datos DNS, sino que los FIRMA digitalmente para ser validados por los recursivos.
- Agrega registros DNS a los ya conocidos (SOA, A, NS…) DNSKEY-RRSIG-NSEC-DIS.

La vulnerabilidad mencionada (*Efecto Kaminsky*) se está contrarrestando a través de lo que se llama DNSSEC.

¿Qué es DNSSEC? Es la extensión de seguridad del protocolo DNS, el protocolo del Sistema de Nombres de Dominio. Se diseña para lidiar con el problema del envenenamiento del caché, de forma tal que si yo quiero llegar al sitio web del Banco Nacional, www.bncr.fi.cr, no vaya a llegar a un sitio web falso.

Como lo explicaba al principio, toda la información de los dominios se recibe a través del sitio web www.nic.cr. Posteriormente registramos en el servidor de nombres primario todos los nombres de dominio con sus servidores de nombre y direcciones IP. Esta información es la que anunciamos en Internet para que los sitios web sean visibles.



¿Qué es lo que va a hacer la tecnología DNSSEC? Va a firmar digitalmente los registros que están en el servidor primario de nombres, agregando registros adicionales que van a ser validados por los servidores recursivos. Así, estos servidores validarán que la información que están recibiendo no fue cambiada y que es la información que está en el servidor primario de nombres. Lo anterior va a contribuir a que cuando una persona digite www.bncr.fi.cr sea llevada a la página correcta y no a una página falsa. La tecnología DNSSEC trabaja con el concepto de llave pública y llave privada.

DNSSEC es una tecnología que debe ser implementada desde la raíz del Sistema de Nombres de Dominio hasta los titulares de los nombres de dominio. Nosotros implementaremos la tecnología en la zona .cr que es la que se nos delegó para administrar. En algún momento los tenedores de dominio también firmarán la zona que se le delegó, por ejemplo la Universidad de Costa Rica firmará ucr.ac.cr. También va a ser necesaria que la raíz que es administrada por el ICANN (Internet Corporation for Assigned Names and Numbers) sea firmada.

La firma por las partes anteriores es necesaria para que exista una cadena de verificación. Si solo una parte firma, es un avance pero no es lo que se requiere para evitar ser enviados a páginas web falsas por el envenenamiento del caché. También se va a requerir que los proveedores de acceso a Internet y administradores de servidores recursivos tengan activa la validación DNSSEC.

- No soluciona todos los problemas de seguridad, pero es útil para proteger el directorio de búsqueda.
- NIC Costa Rica inició investigación en el 2008, se trabaja para implementar en el 1er. Semestre del 2010.

La implementación DNSSEC en la que estamos trabajando, se espera se realice a inicios del otro año (2010), firmando nuestra zona (.cr). Posteriormente vendrá un trabajo con nuestros clientes para que firmen sus zonas, y un trabajo adicional con los proveedores de Internet de nuestro país, capacitándolos sobre que es la herramienta, como funciona y cuáles son los cambios que tienen que hacer en su infraestructura, para que la tecnología pueda tener la utilidad prevista.

La pequeña empresa entiende que la seguridad es importante

Nicolás Severino

Hoy en día, la seguridad es un tema que se ha vuelto cada vez más importante, no sólo en el plano físico, sino también en el informático. Antes, los atacantes buscaban crear virus o amenazas que impactaran a muchos usuarios, que se hiciera mucho ruido, pero ahora los ataques son muy diferentes y, cuanto más silenciosos, dirigidos y exitosos sean, mejor. Lo que los ciberdelincuentes buscan ya no es fama, sino obtener ganancias financieras, lo que ha dado origen a una economía clandestina en Internet en donde se comercializan datos e información de todo tipo.

Con este cambio, hemos visto que lo que los robos de información han aumentado y los ciberdelincuentes buscan ahora objetivos como propiedad intelectual, tarjetas de crédito, claves de cuentas bancarias y claves de acceso de correo electrónico (de correo electrónico

porque mucha gente usa la misma clave para todo y además por el factor de tener una cuenta activa, confiable y obtener nuevos contactos) que les permitan obtener beneficios financieros(ver gráfica 1).

Gráfica 1

Precios de objetos comercializados en la Economía Clandestina

Ranking 2009-2008		Producto	Porcentaje 2009-2008		Rango de precios (Dólares) Americanos)
1	1	Información de tarjeta de crédito	19	19	$ 0.85-$ 30
2	2	Claves de cuentas bancarias	19	32	$ 15-$ 850
3	3	Cuentas de correo	7	5	$ 1 $-20
4	4	Dirreciones de correo	7	5	$ 1.70/MB-$ 15/MB
5	9	Scripts shell	6	3	$ 2-$ 5
6	6	Identidades completas	5	4	$ 0.70-$ 20
7	13	Dumps de tarjeta de crédito	5	2	$ 4-$ 150
8	7	Mailers	4	3	$ 4-$ 10
9	8	Servicios de cash-out	4	3	$ 0-$ 600 plus 50%-60%
10	12	Cerdenciales de administración de sitos Web	4	3	$ 2-$ 30

Fuente: Informe sobre las Amenazas a la Seguridad en Internet (ISTR) Volumen XV, Symantec 2010

De acuerdo con datos del más reciente Informe sobre Amenazas a la Seguridad en Internet de Symantec, la mayoría de los ataques están aprovechando la abundancia de información personal abiertamente disponible en los sitios de redes sociales, para realizar ataques de ingeniería social dirigidos a personas claves de las empresas seleccionadas. Es decir, están dirigiendo la mayoría de los ataques hacia empresas de todos los tamaños quienes tienen y manejan una gran cantidad de información, lo que representa un gran potencial de obtener ganancias económicas de la propiedad intelectual (PI) corporativa atacada.

Esta situación nos ha llevado a identificar que, en realidad, los retos y las necesidades que tienen las pequeñas y medianas empresas en materia de protección, son muy parecidos a los que tienen las grandes empresas. Lo que puede llegar a cambiar entre ambos grupos es la cantidad de información, las regulaciones que manejan y los recursos con que cuentan.

En este sentido, queremos enfatizar que hablamos de protección y no de seguridad, porque protección es algo mucho más completo que no solo se ocupa de un virus o de un robo de información, sino también de que, si por alguna razón se pierde o daña cierta información, se cuente con los procesos y la tecnología necesaria para que las operaciones en la empresa no se detengan y/o se restablezcan lo más pronto posible.

Pensemos por ejemplo en la región del Caribe y los huracanes, una empresa por más pequeña o grande que sea, no puede dejar de facturar o de atender a sus clientes porque pasó un huracán o una fuerte lluvia que afectó su centro de datos, por ello debe montar un esquema de alta disponibilidad de los servicios, y esto es parte de una estrategia de protección que va más allá de un virus.

Amenazas a la seguridad en internet

Las pequeñas y medianas empresas se están convirtiendo en un objetivo popular de los delincuentes electrónicos ya que, a diferencia de las grandes empresas, es probable que no posean infraestructuras de seguridad firmemente consolidadas. Asimismo, los atacantes siguen innovando, y sus formas de atacar son cada vez más complejas, de hecho, de acuerdo con un reporte de Symantec, los atacantes se están moviendo hacia países emergentes y, en América Latina, Costa Rica se ubica en el lugar número 80 a nivel mundial en lo que se refiere al nivel de actividad maliciosa. (ver gráfica 2).

Gráfica 2

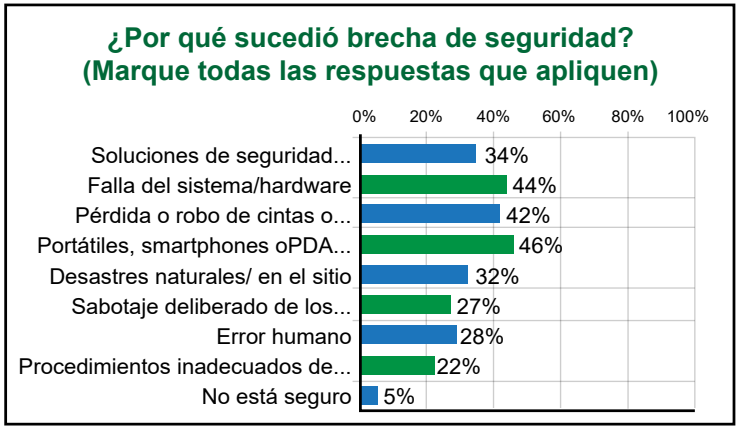
Actividad maliciosa por país (en América Latina)

LAM Ranking 2008	2009	País	Porcentaje 2008	2009	Ranking 2008 2009 por Actividad Código malicioso	Spam zombies	Phising	Bots
1	1	Brasil	43	34	1	1	1	1
2	2	México	13	17	2	4	4	5
3	3	Argentina	13	15	6	2	2	2
4	4	Chile	7	8	5	5	3	3
5	5	Colombia	7	7	4	3	5	6
6	7	Venezuela	3	3	3	9	6	10
7	6	Perú	3	4	7	6	8	4
8	9	Republica Dominicana	1	1	11	7	19	7
9	8	Puerto Rico	1	2	9	12	10	8
10	12	Uruguay	1	1	24	8	9	12

Fuente: Informe sobre las Amenazas a la Seguridad en Internet (ISTR) Volumen XV, Symantec 2010

Por otra parte, de acuerdo con los resultados de una encuesta sobre Seguridad y Almacenamiento en las PyMEs realizada por Symantec en 2009, aproximadamente una de cada tres pequeñas y medianas empresas en América Latina ha enfrentado una brecha de seguridad en los últimos doce meses, lo que significa que información importante o confidencial de la compañía se perdió, ha sido robada o consultada sin autorización. En gran medida, estas brechas se deben principalmente a gallas en el sistema, el robo o pérdida de medios de almacenamiento y de medios portátiles como laptops, smartphones o PDAs.

Gráfica 3
Objetivos de Seguridad en las PyMEs



Fuente: Encuesta 2009 sobre Seguridad y Almacenamiento en las PyMEs, Symantec 2009

La misma encuesta, realizada en la primera mitad de 2009 entre 1,425 pequeñas y medianas empresas (10-500 empleados) en todo el mundo (300 de ellas en mercados de América Latina como Argentina, Brasil, Colombia y México), señala que las tres principales preocupaciones en materia de seguridad que enfrentan las PyMEs en la región son los virus (77 por ciento), las fugas de datos (73 por ciento), y el control y la protección de dispositivos portátiles que se conectan a la red de forma remota (72 por ciento).

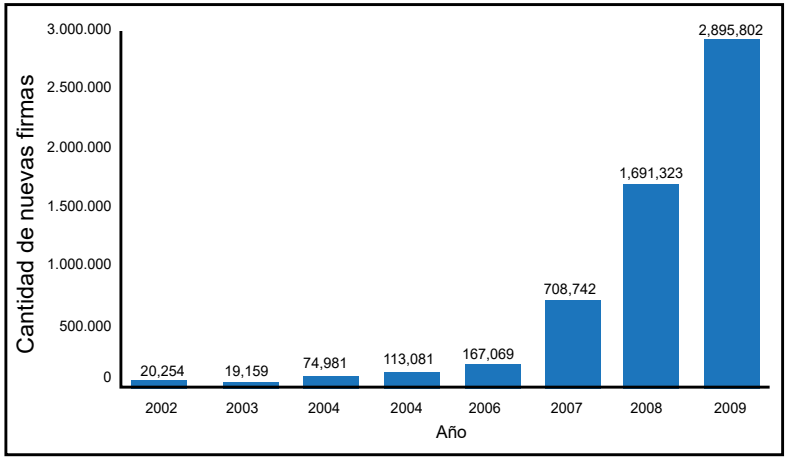
Es decir, las pequeñas y medianas empresas de América Latina parecen estar conscientes de la importancia de la seguridad para sus organizaciones, pero más de la mitad no ha implementado alguna solución de protección de endpoints que les permita proteger sus datos confidenciales contra los distintos riesgos para evitar fugas de datos. Esto hace que exista una discrepancia entre lo que se dice y lo que se hace. Mientras tanto, las amenazas a la seguridad siguen creciendo en complejidad, cantidad y frecuencia, y lo mismo pasa con la cantidad de información, por ello, las PyMEs y las empresas de cualquier tamaño deben implementar estrategias y soluciones para proteger y administrar su información adecuadamente.

Sin embargo, en materia de protección, hemos identificado que las PyMEs enfrentan algunos obstáculos. Los principales son en el tema de la calificación y habilidades de su personal, la falta de tiempo para realizar estas tareas y los presupuestos o recursos con que cuentan.

En cuanto a las amenazas que enfrentan, de acuerdo con la décimo quinta edición del Informe sobre Amenazas a la Seguridad en Internet de Symantec, es claro el incremento en ataques, especialmente en las tácticas diseñadas para facilitar el delito en el ciberespacio. Tan solo el año pasado, Symantec bloqueó en promedio 100 ataques potenciales por segundo y se identificaron más de 240 millones de nuevos programas maliciosos, un aumento de 100 por ciento respecto a 2008(ver gráfica 4).

Gráfica 4

Crecimiento de Códigos Maliciosos



Fuente: Informe sobre las Amenazas a la Seguridad en Internet (ISTR) Volumen XV, Symantec 2010

De las amenazas que las técnicas de Symantec basadas en reputación lograron proteger para los usuarios en 2009, un 57 por ciento fue de instancias únicas. Además, como resultado de esto, la información comprometida siguió creciendo y 60 por ciento de todas las fugas de datos que expusieron identidades de usuarios, fueron resultado del hakeo.

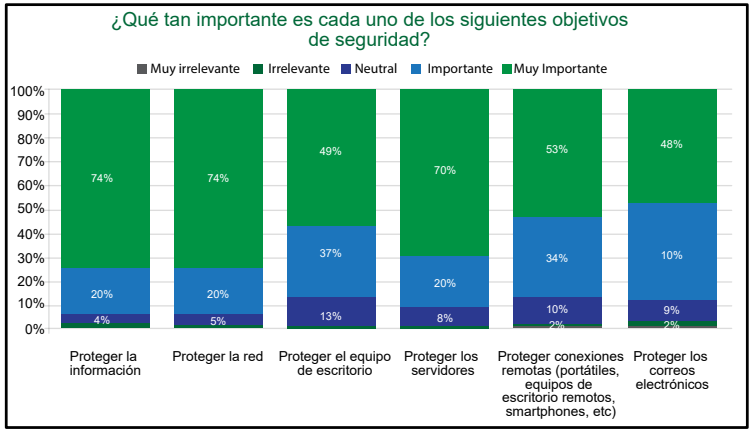
Sabemos que los negocios exitosos de hoy dependen de la tecnología, de la información y de los datos almacenados electrónicamente, por ello es imperativo implementar soluciones de seguridad confiables y apalancar esta iniciativa con políticas de seguridad. La base para garantizar la óptima operación de toda compañía es la integridad de la información, es decir, respaldo, protección y disponibilidad de la misma.

Cabe destacar que especialmente en el caso de la pérdida de información, es básico que todas las pequeñas y medianas empresas, así como corporativos y usuarios residenciales, hagan un análisis de cuánto tiempo y dinero les costaría la pérdida de una base de datos, de sus correos electrónicos y de cualquier información vital dentro de su organización, para posteriormente implementar políticas y soluciones que les permitan mantener a salvo sus datos.

Objetivos de protección de las PyMEs

De acuerdo con la encuesta de Symantec realizada entre 1,424 PyMEs en todo el mundo, los objetivos fundamentales en materia de protección en este tipo de empresas están relacionados con proteger la información, la red, los servidores y los equipos de escritorio (ver gráfica 5).

Gráfica 5
Objetivos de Seguridad en las PyMEs



Fuente: Encuesta 2009 sobre Seguridad y Almacenamiento en las PyMEs, Symantec 2009

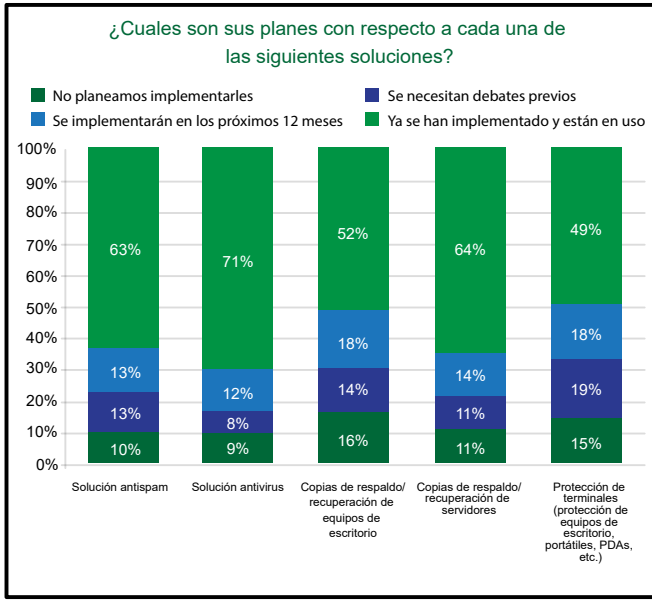
¿Cuál es el factor común entre estas tres cuestiones? Que en todos los casos se ve involucrada la propiedad intelectual de la compañía, lo más importante, lo que las diferencia del resto.

La seguridad y las PyMEs

Aunque las PyMEs entienden los riesgos de seguridad que enfrentan, una cantidad sorprendente de estas empresas en América Latina no cuenta con prácticas elementales de seguridad. De hecho, un 29 por ciento de las pequeñas y medianas empresas encuestadas en la región no tienen la protección más básica – un antivirus. Además, como lo muestra, un 36 por ciento no tiene instalada una solución antispam y 52 por ciento no ha implementado una solución de protección de endpoints (software que protege equipos portátiles, de escritorio y servidores contra *malware*).

Gráfica 6.

Adopción de Soluciones de Protección en las PyMEs

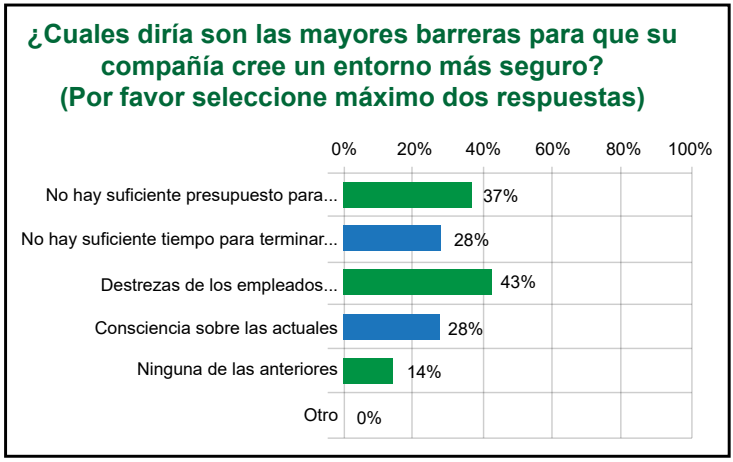


Fuente: Encuesta 2009 sobre Seguridad y Almacenamiento en las PyMEs, Symantec 2009

Sin embargo, existen algunas razones que hacen que las PyMEs de América Latina no estén protegiendo totalmente la información confidencial de su compañía. Entre las principales barreras para crear un entorno más seguro, Symantec identificó cuatro respuestas principales: 43 por ciento de las PyMEs dijo que había una carencia de habilidades por parte de los empleados, 37 por ciento mencionó que sus presupuestos limitados eran un impedimento para realizar todas las labores relacionadas con la seguridad y 28 por ciento citó el tiempo y la falta de conciencia sobre las actuales amenazas a la seguridad de TI como un obstáculo. (ver gráfica 7).

Gráfica 7.

Principales Barreras para las PyMEs



Fuente: Encuesta 2009 sobre Seguridad y Almacenamiento en las PyMEs, Symantec 2009

Así que, aunque dos tercios de las PyMEs en América Latina tienen empleados de TI dedicados a labores relacionadas con los sistemas informáticos, las PyMEs citaron las habilidades de los empleados y los cortos presupuestos como las principales razones que les impiden proteger sus recursos de TI y su información. Sin embargo, el costo de no prevenir una fuga de datos la mayoría de las veces supera los costos que ésta podría generar, por ello es importante que las PyMEs

implementen una estrategia sólida de seguridad que incluya políticas eficaces, desarrollo de habilidades y soluciones de seguridad integral.

Con el aumento de la cantidad y la sofisticación de virus basados en la Web y códigos maliciosos, las pequeñas empresas deben estar protegidas con algo más que la tradicional tecnología antivirus. Por ello, si las pequeñas empresas combinan políticas efectivas de seguridad con mejores prácticas y una solución que ofrezca una protección multicapas que incluya *antivirus, antispam, firewall, IPS, IDS*, entre otros, las pequeñas empresas estarán a salvo y podrán confiar en su seguridad y centrarse en la operación y el crecimiento de su empresa.

Más información en: www.symantec.com/es/mx/business/solutions/smallbusiness

Recomendaciones para determinar el nivel de protección en la pequeña y mediana empresa

- Examine el sistema existente para determinar la exposición de la seguridad y cómo minimizar estos riesgos.
- La red: ¿qué clase de protección utiliza actualmente? ¿Qué clases de conexiones se realizan en la red? ¿Algún emplea do se conecta de forma remota?
- Dispositivos utilizados: ¿cuántos y qué clases de dispositivos se conectan a la red? Por ejemplo, la seguridad inalámbrica se trata de forma diferente a la seguridad de los dispositivos con cable. ¿Qué clase de seguridad se está utilizando ahora?
- Activos de información: ¿cuáles son los datos e información confidenciales de la empresa, y dónde se guarda? La información valiosa requiere un cuidado especial de seguridad.
- ¿Quiénes son los usuarios? - Piense en quién puede acceder a qué información en la red, y cuáles son las clases de contraseñas que se requieren.
- Creación de un plan de seguridad.
- Cada empresa, independientemente del tamaño de la red, debe poseer un plan de seguridad. Recuerde que un plan de seguridad debe definir el comportamiento adecuado del

usuario e identificar los procedimientos y las herramientas de seguridad que se implementarán.

- Los temas importantes que debe incluir en el plan de seguridad: derechos de acceso: una empresa puede optar entre tres opciones cuando se trata de la confianza: 1) confiar en todo el mundo en todo momento; 2) desconfiar de todo el mundo en todo momento; 3) confiar en algunas personas, a veces. Cada enfoque tiene sus ventajas y desventajas, pero la tercera opción es el modelo empresarial más común.
- Acceso remoto: un plan de seguridad debe establecer prácticas informáticas seguras para los usuarios remotos. Esto incluye el uso del antivirus y del *firewall* en los dispositivos informáticos, y cómo realizar una conexión VPN segura.
- Protección de la información: detalle directrices para procesar, almacenar y enviar los activos de TI confidenciales de la empresa.
- Prevención de virus: reduzca la exposición a virus con *software* de seguridad y educación del usuario. Señale las soluciones de seguridad necesarias en la red, el perímetro y la estación de trabajo. Suministre a los usuarios un ma nual sobre prácticas informáticas seguras.
- Uso de contraseñas: requiera que los usuarios cambien las contraseñas con frecuencia por contraseñas alfanuméricas de ocho dígitos.
- Copia de respaldo y recuperación: realice copias de respaldo periódicas de los datos importantes. Cree un plan para recuperar los datos en caso de alguna interrupción en la red.

La seguridad administrada y la gestión de la seguridad

Luis Cerdas Ross

En el año 1999 tuve la oportunidad de fundar una empresa especializada en brindar soluciones de seguridad informática y la protección de la información. Actualmente, como Director de Operaciones de Seguridad de Managed Security Agency, S.A. (MSA®) empresa dedicada a proveer servicios de seguridad administrada, asesoría y soporte continuo, una de mis labores principales es ayudarle a nuestros clientes a identificar el valor de su información y diseñar políticas y controles tecnológicos para su protección, para luego poder implementar un ciclo permanente de implementación, valoración y mejoramiento.

Este proceso comienza estableciendo un denominador común de conocimiento sobre los conceptos básicos de la seguridad informática y el por qué es necesario tomarla en cuenta, la importancia de la gestión de la seguridad dentro de la empresa y finalmente, las opciones existentes para poder adquirir e implementar una solución de seguridad administrada exitosa.

Conceptos básicos

El renombrado investigador, Don B. Parker definió a la seguridad informática como la búsqueda para maximizar la confidencialidad, la integridad, la disponibilidad, la autenticidad, la utilidad y mantener la posesión y el control de la información. (Parker, Donn B. (2002) "Toward a New Framework for Information Security" Bosworth, Seymour; Kabay, ME The Computer Security Handbook (4th ed.).

Existen otras definiciones que en MSA® consideramos son incompletas o bien, se prestan para confusiones y para crear falsos sentidos de seguridad al no contemplar las diferentes aristas pertinentes.

La confidencialidad se refiere a los límites que se pueden establecer sobre quién tiene acceso a la información. Como ejemplo, los detalles sobre las negociaciones entre empresas aliadas no deberían ser conocidos por sus competidores; el grado de control sobre quienes tengan acceso a dicha información es el grado de confidencialidad de la misma.

La integridad se refiere a la consistencia y a lo completo de la información. Cualquier alteración no autorizada, ya sea con dolo o accidental, afecta directamente la integridad de la información. Esto puede ser un estudiante que modifica sus notas en el servidor del colegio, un delincuente que cambia el saldo en una cuenta bancaria o simplemente una falla en la capa magnética del disco duro que corrompe un archivo.

La autenticidad hace referencia a la veracidad del orígen o autoría de la información. En múltiples ocasiones se convierte en algo crítico el poder establecer de forma fidedigna el origen de la información; en su forma más simple, se trataría de la identidad de la persona con la que se intercambia un correo electrónico o un sitio web con el que se realizan transacciones comerciales.

Disponibilidad significa tener acceso a la información de forma oportuna. Si un equipo con información falla por cuestiones de electricidad, conectividad o intervención humana, el no poder accesar esa información impacta de forma negativa a la organización. Puede referirse al acceso a información comercial como precios y ofertas, a herramientas de trabajo como el correo electrónico y

calendarios o bien, clientes que no pueden comprar sus productos ni acceder a sus servicios.

Utilidad significa poder hacer uso de la información. El ejemplo más simple de este concepto es tener la información requerida almacenada en un medio al cual no se puede acceder. Por ejemplo, un archivo urgente cuya única copia se encuentra en un *diskette* (o peor aún, en una cinta magnética) y todos los equipos de cómputo de la empresa no tienen el *hardware* necesario para accesarlo. Aunque la información requerida cumple con los elementos anteriores, no se puede hacer uso de la misma.

Una vez que se cuenta con un claro entendimiento de los conceptos anteriores, resulta mucho más fácil poder entender que la información puede ser afectada de diversas formas y que por lo tanto existen múltiples formas de protegerse. Parte de la problemática actual en cuanto al aseguramiento de la información y a la seguridad informática es que se ha creado un sentimiento general de confort al contar con un único control (ya sea un muro de fuego, un anti virus, etc.). Se cree que ya con eso basta, y como vamos a ver, este es un grave error.

La seguridad informática, vital en el mundo contemporáneo

Nuestra sociedad ha evolucionado hasta el punto en que la tecnología y el manejo de la información permean la vida de todas las personas, aún aquellas que nunca en su vida han tocado una computadora. Desde que nacemos estamos inscritos en bases de datos del gobierno; al adquirir servicios públicos nuestra información alimenta y se almacena en diferentes equipos y sistemas de bases de datos; si poseemos cuentas bancarias para recibir el salario, ahorrar o acceder a créditos, nuestra información se propaga a otros, incluyendo empresas "protectoras" de crédito y hasta tiendas de electrodomésticos.

Toda esta información debe ser protegida para cumplir con al menos un mínimo de seguridad en su manejo y gestión. En estos casos no se tiene mucha más opción que esperar que todas esas entidades sepan salvaguardar la información y que designen los recursos necesarios para minimizar los riesgos existentes.

Pero, ¿qué pasa cuando la responsabilidad del manejo de la información es propia y no de un tercero? .Todos manejamos información de otras personas, la mayoría sin darse cuenta de la importancia de la información que se maneja. Empresas e instituciones de todo tamaño, grandes y pequeñas, almacenan números de tarjetas de crédito y de cuentas bancarias, teléfonos y nombres de clientes, listas de precios de proveedores y códigos de acceso para cuentas de correo electrónico, banca electrónica y sitios web. A título personal, tenemos fotos y correos de familiares en nuestras computadoras, números de teléfono privados, fotos y videos en los teléfonos celulares.

El caso se complica aún más cuando se ofrece información y productos para la venta a través de Internet y cuando las herramientas como el correo electrónico y los documentos digitales pasan a ser de uso diario y obligatorio. Actualmente cada equipo conectado directamente a Internet recibe al menos sesenta ataques e intentos de acceso no autorizado cada hora. Este número se incrementa a más de cuarenta ataques por minuto en casos de ataques automatizados de fuerza bruta.

Estos ataques no diferencian entre bancos, instituciones de gobierno o pequeñas y medianas empresas, personas navegando desde su casa o desde su teléfono celular. Todos están expuestos y en su mayoría, están muy vulnerables sin siquiera saberlo. No podemos pasar por alto el llamado urgente a tomar control de nuestra información, ya sea que esta esté en nuestras manos o en las de un tercero "de confianza." Vivimos en un mundo digital donde realizamos transacciones electrónicas, nos comunicamos a larga distancia y trabajamos con sistemas electrónicos. Pero, ¿cómo tomamos este control?

La gestión de la seguridad de la información

La única forma de tomar control de nuestra información es por medio de la gestión de la seguridad de la información. Este es un proceso que incluye la identificación y la categorización de la información (saber cuál es la información y qué tan importante es); la definición

de políticas empresariales sobre el manejo de la información; el alineamiento de estas políticas con la estrategia empresarial; y finalmente, el ciclo de implementación, valoración y mejoramiento.

Toda entidad, sin importar su tamaño, ya sea gubernamental o empresa privada, debe implementar programas para la gestión de la seguridad de su información. Esto es de suma importancia estratégica y, como tal, involucra directamente a las máximas gerencias y directivos. Es frecuente encontrar que, erróneamente, esta responsabilidad se le delega a los departamentos de informática sin asignarles los recursos necesarios y sin involucrar a las otras áreas de la institución, lo que genera un falso sentido de seguridad, problemas entre departamentos y sobrecarga del personal de informática.

Lo que entonces sucede es que los departamentos de informática usualmente no cuentan con el presupuesto necesario, ni el recurso de personal con conocimiento especializado de forma dedicada, ni tampoco con la autoridad para poder implementar las políticas requeridas para el aseguramiento de la información. Un departamento de informática no puede (ni debe) dictar las políticas de seguridad de la información. La responsabilidad que sí puede asumir es la implementación de los controles necesarios para aplicar y hacer cumplir las políticas que la dirección de la empresa defina.

El por qué esto es una cuestión de índole de estrategia empresarial y no "un problema de informática" tiene respuesta en los múltiples elementos que se deben tomar en cuenta al formular un plan integral para la gestión de la seguridad. Una política aparentemente simple, como "se prohíbe el acceso a la pornografía" conlleva el análisis obligatorio de aspectos de recursos humanos (como la forma de notificar la política a los colaboradores), legales (como las posibles consecuencias para los infractores y la entidad en caso de demandas por aquellos a quienes se les aplique un posible castigo), tecnológicos (el diseño e implementación exitosa de los controles necesarios para poder hacer respetar la política de forma confiable y consistente) y hasta cuestiones de índole teórico ("¿qué es pornografía?") que deben ser definidas de forma clara y como parte de la identidad de la empresa o institución. Los riesgos que deben considerarse van

desde un simple robo de un equipo de cómputo o teléfono celular, hasta la posible intervención de las comunicaciones, la alteración de datos o la pérdida de control de las herramientas de Internet, como el correo electrónico o la presencia en la Web.

Todos estos riesgos requieren ser considerados desde una perspectiva empresarial y su impacto en el negocio y el funcionamiento de la entidad. ¿Qué pasa si no tenemos correo electrónico? ¿Qué pasa si un competidor consigue una copia de nuestros costos o de los precios que nos dan nuestros proveedores? ¿Qué hacemos para poder vender, si no hay electricidad? ¿Si prohibimos el acceso a ciertos sitios web, qué pasa si nos demanda un colaborador?

Por qué es importante contar con profesionales para la gestión de la seguridad

Aunque puede parecer muy complicado establecer los lineamientos necesarios para el manejo de la seguridad de la información, esto se facilita enormemente si se cuenta con un profesional experimentado y dedicado a la gestión de la seguridad. Este se convierte en el responsable de promover, coordinar y supervisar el desarrollo y la implementación de un programa para la gestión de la seguridad.

Esta persona tiene la responsabilidad fundamental de integrar los esfuerzos de los diferentes elementos involucrados, tanto internos como externos, para poder implantar un ciclo empresarial de identificación, mitigación y gestión continuo, acorde a la estrategia global de la empresa. Evidentemente esta persona no puede ni debe realizar todas las acciones necesarias para que todo esto funcione. Para eso se requiere involucrar a personal de múltiples disciplinas y áreas de la entidad.Aquí es donde la institución tiene la posibilidad de apoyarse en aquellos recursos internos o externos que posean el conocimiento y la experiencia para poder asesorar, diseñar e implementar las políticas y los controles tecnológicos y operacionales necesarios de forma exitosa.

Designar recursos dedicados, tales como establecer el puesto del responsable de la gestión de la seguridad, resulta difícil en las entidades medianas y casi imposible en las pequeñas debido a los costos

que esto significa, los cuales van desde salarios y remuneración hasta la capacitación continua para el personal.

Debido a esto, aún en las entidades de mayor tamaño, en conjunto con la asignación de las responsabilidades de seguridad a los departamentos de informática, se genera un vacío que deja expuesta la misma información que se quiere y debe proteger. Este vacío se puede llenar exitosamente contratando el correcto servicio de seguridad administrada.

Seguridad Administrada

Diferentes tipos de Seguridad Administrada y qué le conviene a cada tipo de empresa

La seguridad administrada es un modelo operacional que le permite a las empresas e instituciones contratar a un aliado estratégico para apoyar su gestión de la seguridad de la información, ya sea para asesorar en el lineamiento estratégico gerencial, para co-administrar la gestión de seguridad desde políticas operacionales hasta la configuración y el mantenimiento de equipos y dispositivos o bien, para asumir la gestión completa como un servicio de *outsourcing* de todas las funciones y responsabilidades asociadas.

A través de estos servicios, las entidades pueden tener acceso a personal, equipo y conocimiento altamente especializados de forma flexible y continua según sus necesidades sin tener que desarrollar la infraestructura y realizar las inversiones internas.

Actualmente se pueden detallar tres tipos de seguridad administrada: En primer lugar, encontramos a aquellos proveedores que se dedican a administrar un gran volumen de dispositivos de todo tipo, incluyendo equipos de comunicaciones, de cómputo y de seguridad. Su enfoque está en poder incluir el mayor número de dispositivos y así contar con una cartera identificada por la cantidad de equipos administrados. Frecuentemente cuenta con centros de llamadas extensos y con personal técnico rotativo para atender los posibles incidentes con los múltiples dispositivos de los clientes.

Este modelo de administración funciona bien para aquellas entidades que poseen un departamento interno dedicado a la gestión de la seguridad de la información; cuentan con un puesto para el responsable de la gestión de la seguridad y requieren, por cuestiones de costos, reducir la carga adicional que la administración de todos estos dispositivos significa para el área de informática.

En un punto intermedio se encuentran aquellos proveedores que tradicionalmente se han dedicado a la venta de productos tecnológicos, tales como equipo de cómputo y *software* de toda índole, que han reconocido que existe un negocio lucrativo en el mercado de la seguridad informática y, por lo tanto, la han integrado como parte de su cartera de productos. La seguridad es un apéndice que surge de una oportunidad y no como su razón de ser.

El último modelo busca llenar el vacío de conocimiento y recursos que les impide a las instituciones y entidades reconocer sus necesidades de seguridad de la información y poder hacer algo para atenderlas y minimizar el riesgo e impacto de incidentes para que, sin importar su tamaño, puedan gozar de una seguridad personalizada.

Para brindar un verdadero servicio profesional utilizando este modelo, se debe contar con la experiencia y el personal correcto; el conocimiento profundo, más allá de las cuestiones técnicas, es de suma importancia, incluyendo el manejo de la legislación penal y laboral aplicable y cuestiones de gestión de recursos humanos, que son críticos para dar la asesoría esperada. Pero además, para poder implementar y soportar los controles tecnológicos que apoyan las decisiones gerenciales, se debe contar con el conocimiento técnico y amplia experiencia en el diseño, el manejo, la configuración y la administración de múltiples dispositivos de seguridad en ambientes heterogéneos.

Cómo contratar a un proveedor de seguridad administrada

En primera instancia, debe reconocerse la importancia de proteger la información que se maneja dentro de la empresa o institución, y esto como un requisito para el éxito y no como una obligación. Si no existe voluntad (o interés) para proteger la información o se

relega la gestión de la seguridad a un plano secundario, cualquier intento de implementar controles de seguridad integrados fracasará y posiblemente, de forma desastrosa y muy perjudicial. Tener un "anti-virus" o un muro de fuego ("firewall" en inglés) no es suficiente. No están protegidos. Hasta que eso no se entienda, cualquier esfuerzo adicional será en vano.

Seguidamente, se deben identificar y clasificar los tipos de información que maneja la entidad y de ser posible, los diferentes métodos de acceso, almacenamiento y uso que se le brinda a la información. Con esto listo, la entidad puede establecer un pliego de requisitos y condiciones para recibir ofertas y poder seleccionar los candidatos idóneos para brindar el servicio.

En cuestiones de seguridad es importante tomar en cuenta que la información en sí es sumamente valiosa y que precisamente por ese valor intrínseco es que se debe proteger. Por lo tanto, no es prudente hacer público los diseños, la arquitectura e implementación de los dispositivos de control de la seguridad. En el caso de las empresas privadas, basta con ejercer la confidencialidad del caso, pre-seleccionar proveedores y limitar el acceso a información sensitiva.

En el caso de las instituciones públicas, la Ley de la Contratación Administrativa ha previsto exactamente esta situación y la Contraloría General de la República ha reconocido en múltiples ocasiones, la correcta aplicación de la "excepción por seguridad calificada" en los procesos de contratación. Es importante notar que dicha excepción no puede ser invocada solo por tratarse de un producto de seguridad, sino que debe de existir un posible daño evidente si dicha información se hiciera pública.

Como ejemplo, una institución que desea adquirir un sistema de monitoreo por circuito cerrado con múltiples cámaras puede realizar una contratación por excepción de seguridad calificada para el diseño de la red de monitoreo (ubicación de cámaras, cuarto de control, requerimientos de almacenamiento del video, etc.); y luego una compra por concurso público para adquirir el equipo según la arquitectura diseñada. La compra pública establece los requerimientos de funcionalidad,

materiales y de servicios, tales como localidades a instalar, cantidad de cableado, tipos de sensores, etc., más no así su ubicación dentro de los edificios y sectores.

Otro ejemplo es la adquisición de armas de fuego por parte de la fuerza policial. La compra de un lote de armas de fuego no cumple con los requisitos necesarios para aplicar la excepción por seguridad calificada. La información, en manos de un criminal, sobre el modelo de arma de fuego adjudicado por medio de concurso público no pone en riesgo a la policía que la utilice. Diferente es el caso de la contratación de un servicio de valoración y capacitación sobre procedimientos para el manejo de situaciones de rehenes. Si en el pliego de contratación se detalla el procedimiento actual (o el que se desea aprender) y esta contratación no se protege invocando la excepción de seguridad calificada, un criminal puede planear un secuestro de rehenes conociendo el procedimiento y las tácticas que serían utilizadas en su contra paso a paso, poniendo en riesgo al equipo policial.

Se debe poder comprobar que el personal del proveedor cuenta con experiencia comprobada en la prestación de servicios de seguridad administrada y que dicho personal está comprometido contractualmente con el proveedor para brindar los servicios requeridos a sus clientes. De ser posible, se debe verificar que existen procedimientos y condiciones contractuales para la transferencia de conocimiento del personal clave hacia el personal nuevo del proveedor o bien, al personal pertinente del cliente.

Por todo lo anterior, se debe tomar en cuenta que la compra de productos de seguridad, tales como *software* anti-virus, detectores de intrusos, muros de fuego y renovaciones de licencias de *software* de seguridad no son candidatos aptos para invocar la excepción por seguridad calificada. Por el contrario, la asesoría, la administración y el mantenimiento continuo de políticas de seguridad y su implementación según se requiera dentro de la topología de la entidad sí es un caso recomendado para utilizar la excepción de seguridad calificada. Solo imaginen un pliego de condiciones que establece claramente las políticas implementadas, ¡incluyendo accesos, permisos, horarios, nombres de usuarios, modelos de equipos y su ubicación! Un *hacker*

se estaría ahorrando horas, sino días, de trabajo de investigación y la entidad no solo estaría expuesta, sino que perdería la posibilidad de identificar intentos de ataques que ya el *hacker* no probaría al saber que son innecesarios.

Conclusiones

A fin de cuentas, todas las entidades, ya sean empresas privadas o instituciones públicas, pequeñas o grandes, deben reconocer el valor de su información y luego, entender la forma en que la misma se maneja y transfiere dentro y fuera de la entidad.

Cualquier esfuerzo para implementar controles, tales como muros de fuego y *software* de antivirus, serán en vano o bien, parches desintegrados incapaces de hacerle frente a mayores problemas y riesgos futuros. Para tener una protección real de la información es primero necesario y urgente alinear las políticas de manejo de información con la visión estratégica de la empresa o institución; establecer programas para la difusión de las políticas y lineamientos y para la capacitación de los colaboradores sobre sus responsabilidades y la visión global de la entidad en cuanto a la información.

Todo esto se facilita cuando se cuenta con la voluntad gerencial y se canaliza a través de una persona responsable por la gestión de la seguridad en la entidad. Sus labores de asesoría, manejo y coordinación con las otras áreas involucradas (legal, recursos humanos, informática, finanzas) permite una mayor flexibilidad en el manejo de presupuestos, financiamiento, capacitación e implementación.

Si se cuenta con el recurso humano dentro de la entidad de forma dedicada, el invertir en el permanente mejoramiento de su conocimiento es requerido para poder hacerle frente a los nuevos riesgos emergentes y a los ajustes necesarios según el desempeño y desarrollo de la entidad.

Al buscar ese recurso humano en un proveedor de seguridad administrada, debe poderse comprobar el conocimiento técnico sobre los productos que serán administrados bajo el contrato de prestación de servicios, la experiencia en situaciones similares (respetando la confidencialidad del caso) y los servicios que este proveedor puede ofrecer.

Esto significa que los ingenieros asignados a la atención de los dispositivos cubiertos por el contrato deben contar con las certificaciones pertinentes, al menos del fabricante de los productos, que acrediten su capacidad de administrar y brindar soporte de los productos. El equipo del proveedor de seguridad administrada no debe estar limitado a técnicos e ingenieros informáticos sino que debe estar conformado por profesionales en múltiples áreas empresariales, como mínimo un equipo legal que conozca de derecho laboral e informático y personal capaz de ayudar en la identificación y definición de riesgos y posible impacto en el funcionamiento del negocio.

De esta forma, el proveedor de seguridad administrada se encuentra en capacidad de asesorar al equipo gerencial en el proceso del ciclo de la gestión de la información, cumpliendo parte del rol del gestor de seguridad de la información; en aquellas empresas que tienen a alguien asignado internamente como gestor de seguridad, el proveedor pasa a formar parte esencial del equipo promotor y de implementación y asesoría durante la vigencia de la relación.

El conocimiento íntimo del funcionamiento y la idiosincrasia de cada cliente le permite al proveedor de seguridad administrada establecer medidas personalizadas para cada uno, en lugar de procedimientos genéricos ajustados a la fuerza.

El tener éxito en los negocios y en la prestación de servicios requiere tener claridad en sus propias fortalezas y saber cómo lidiar con las amenazas presentes y futuras. La información empresarial e institucional es una de las mayores fortalezas presentes y que frecuentemente no es tratada como tal. Su protección debe ser uno de los objetivos primordiales de aquellos responsables por el éxito general de la entidad.

MSA®, cuenta con más de diez años de experiencia especializada en la prestación de servicios de seguridad administrada y en el aseguramiento de la información. Nuestro equipo está compuesto por profesionales expertos en la gestión de la seguridad, en la implementación de los controles tecnológicos y especialistas en los aspectos legales y empresariales asociados.

Capítulo 10
Casos de seguridad informática

Protección de datos en el Gobierno Digital

Alicia Avendaño Rivera

La tecnología introdujo un nuevo elemento: "…La identificación del límite sobre la tenencia y utilización de datos personales así como sobre el tráfico de los mismos, es necesario facilitar al ciudadano el derecho a conocer quién está utilizando sus datos personales y para qué, y negar el permiso sobre el uso de sus datos a quien considere oportuno…."

Protección de datos

El concepto de Protección de Datos se relaciona con el *derecho a la intimidad.* "El amparo debido a los ciudadanos contra la posible utilización por terceros, no autorizada, de sus datos personales susceptibles de tratamiento automatizado, para de esta forma confeccionar una información identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad."

El concepto de Protección de Datos se relaciona con el derecho a la intimidad, "el amparo a los ciudadanos contra la posible utilización por terceros no autorizada, de sus datos personales susceptibles de tratamiento automatizado para de esta forma, confeccionar una información que identificable con él, afecte a su entorno personal,

social o profesional, en los límites de su intimidad." Por ejemplo los datos de salud esos datos son personales y deberían mantenerse protegidos a criterio de la persona.

Casos presentados en Costa Rica

Hábeas data es un Recurso Constitucional que consiste en la protección de datos personales, la prohibición de difundir esos datos sin autorización de cada persona, y la inmediata modificación de datos cuando cada individuo así lo establezca.

Con el recurso de *hábeas data* la jurisprudencia de la Sala Constitucional ha evolucionado notablemente desde los fallos de la primera etapa en contra de los archivos criminales administrados por el Organismo de Investigación Judicial. En una de las primeras sentencias se considera el suministro de información es conservado en ese archivo a terceras personas como lesivo al principio de legalidad y a la dignidad de la persona.

Una segunda sentencia se muestra más tímida cuando considera que es posible que ese archivo criminal pueda conservar los registros individuales aun después de su vencimiento. Posteriormente y ya en el orden de fallos más reciente, el voto 4154-97, ya habla expresamente del *hábeas data* y su regulación, planteando que el objeto de este recurso es la protección a conocer o rectificar la información pública o privada que exista sobre ella. Han sacado sentencias inclusive la última sentencia que se sacó, obligó a borrar a estas empresas la dirección suya porque es un dato personal.

El voto1345-99 dos años después abre la posibilidad de una tutela de acceso, con base en el derecho a la auto determinación informativa para que la gente pueda conocer las informaciones que sobre ellas se encuentren allí registradas, e incluye una descripción de los derechos que lo asisten. En un fallo más sistematizado, el 5802-99, la Sala Constitucional entra a analizar el registro y los bancos de datos y los objetivos del *hábeas data*, así como los principios que rigen el ejercicio de estos derechos. Prejuicios que se le causaron a un ciudadano al ser incluido injustamente, sin su consentimiento y sin saberlo, en un listado de morosos de un banco, luego de muchas

gestiones, y más de tres años de no obtener ningún crédito producto de su inclusión en ese listado logró por intermedio del Defensor del Pueblo que se le excluyera de esa lista. Casos como este han de ser muy frecuentes y probablemente son solamente la punta del iceberg de una problemática muy compleja que causa daños a muchos ciudadanos.

Hay unos casos en Costa Rica que han causado que personas que por estar insertos en estas instituciones de riesgo financiero hayan tenido injustamente que padecer la denegación de un crédito, y que luego de tres años sin obtener un crédito por estar en este listado, por medio de la Sala IV se logró que se excluyera.

Hay votos constitucionales. Sobre estos datos personales y se manejan en las instituciones públicas, en algunos casos se reparte la información y en algunos casos se vende. Todos estos datos es lo que ha ayudado a nuestra protección, pero no hay una legislación que nos proteja, nuestra información esta regada por todos lados y no hay protección.

Las protectoras de crédito como Datum, Teletec y Cero Riesgo están en la obligación de borrar de sus bases de datos la dirección domiciliar de quienes así se lo soliciten. Esta semana dos fallos de la Sala Constitucional consideraron que esa es información privada de cada costarricense.

Retos de protección de datos

Precisamente uno de los retos es como estamos viendo y cuál es el diseño aparate de todos los sistemas de seguridad, que es muy importante la renovación y la actualización, pero que a nivel de Estado y de instituciones que debemos hacer trabajo conjunto, porque hasta ahora no se comparte entre instituciones, no hay esquemas de información para compartir.

Parte de lo que hemos buscado nosotros en el Gobierno Digital es como orquestar esa interconexión de los datos, porque en este momento las bases de datos están en el Registro Civil, (el padrón electoral) y en muchas otras bases de datos. A través de Gobierno Digital lo que se quiere es hacer un intercambio coherente de información entre las instituciones. Varios países lo han hecho, tenemos

que ver como lo han hecho porque estamos muy atrasados en el tema de Gobierno Digital o de políticas o esquemas, apenas estamos empezando. En temas como firma digital países como Corea o Singapur tienen 20 años de tener firma digital.

¿Qué es la interoperabilidad?

Conceptos sobre Interoperabilidad: "Intercambio coherente de información y servicios entre sistemas. Debe posibilitar la substitución de cualquier componente o producto utilizado en los puntos de interconexión por otro de especificación similar, sin comprometer las funcionalidades del sistema." (Gobierno del *Reino Unido*);

"Habilidad de transferir y utilizar información de manera uniforme y eficiente entre varias organizaciones y sistemas de información." (Gobierno de *Australia*);

"Habilidad de dos o más sistemas (computadoras, medios de comunicación, redes, *software* y otros componentes de tecnología de la información) de interactuar y de intercambiar datos de acuerdo con un método definido, con el fin de obtener los resultados esperados." *(ISO)*;

"Políticas y especificaciones de interoperabilidad claramente definidas, así como gestión de la información, son claves para mantenerse comunicados por el mundo y alineados con la revolución de la información globalizada" *(e-GIF, Reino Unido).*

En la parte de interoperabilidad son muy importantes estos conceptos si ya lo hizo Reino Unido y Australia y hay definiciones claras porque no hacerlos nosotros y mejorar lo que se ha hecho, eso es parte de un proceso en el que estamos. También tenemos que eliminar una limitación del Estado que es la *tramitología* porque tenemos que pedir un documento o emitir una certificación física, tenemos que ir a la ventanilla de la Caja o del Registro y nos convertimos en mensajeros del Estado, cosa que cambiaría si tuviéramos un sistema de interconexión a la base de datos, además de que nuestra información estaría más segura porque no estaría regada por todos lados.

Consideraciones para lograr la interoperabilidad

- Entendimiento del negocio.
- Información definida con las características requeridas para soportar la misión de las entidades y no soluciones técnicas particulares.
- Reutilización de la información.
- Capacidad de incrementar la utilización de la información sinérgicamente, de tal forma que soporte la administración de la información mediante mecanismos innovadores y creativos que ayude al desarrollo de la misión de las entidades.
- Intercambio de información.
- Identificación de la información que se quiere compartir e intercambiar entre entidades, con el sector productivo y con otros gobiernos.
- Armonización de la información.
- Disponer de un modelo confiable y único para definir los conceptos para el intercambio de información en el Estado Costarricense.

Es muy importante tratar de entender que datos son públicos y que datos son privados, porque hay datos que por más que se quieran intercambiar con otra institución; el Registro Público por ejemplo tiene los datos de las propiedades ellos son los dueños de la información, porque ellos son los que brindan el servicio; para el intercambio de la información y la armonización de la misma hay que establecer estándares para intercambiar de forma segura.

Informaciones semánticas, conceptos y utilizar todos los esquemas y estándares internacionales. Para hacer eso necesitamos definir las políticas, la arquitectura, el gobierno y desarrollo de los sistemas de seguridad, los procesos y definir y capacitar las personas que van a participar.

Marco de interoperabilidad del gobierno

e-Mig: Se define como un conjunto de políticas, estándares y especificaciones técnicas que reglamentan a nivel nacional la utilización de la Tecnología de Información y Comunicación (TIC) en la Interoperabilidad de servicios de gobierno estableciendo las condiciones de interacción entre las instituciones del Estado. En el marco de la interoperabilidad del e -Mig que es donde están todas estas políticas de interconexión para proteger los datos tiene que haber una segmentación preliminar: interconexión seguridad, medios de acceso, organización e intercambio de información.

e-Mig: Interconexión

- Protocolo de Transferencia de Hipertexto;
- Transporte de Mensajería Electrónica;
- Seguridad de Contenido de Mensajería Electrónica;
- Acceso Seguro;
- Directorio;
- Servicios de Nombres de Dominio;
- Notación de e mail;
- Protocolo de Transferencia de Archivos;
- Intercomunicación LAN / WAN;
- Transporte;
- Web Services: SOAP, UDDI e WSDL.

e-Mig: Seguridad

- Políticas técnicas: referencia a NBR ISO/IEC 17799:2005;
- Seguridad de IP (Algoritmos, protocolos, certificación);
- Seguridad de Correo Electrónico;
- Criptografía;
- Desarrollo;
- Servicios de Redes.

e-Mig: Medios de Acceso

(I) Estándares para acceso vía estación de trabajo

- Navegadores *(browsers)*;
- Conjunto de Caracteres e Alfabetos;
- Formato de Intercambio de Hipertexto;
- Archivos tipo: "Documento", "Planilla", "Presentación";
- Archivos do tipo "Banco de Dados (para estaciones de trabajo);
- Intercambio de Informaciones Gráficas e Imágenes;
- Gráficos Vetaríais;
- Archivos tipo "Audio" y tipo "Vídeo";
- Compactación de Archivos en General;
- Geoprocesamiento: para estaciones de trabajo.

(II) Smart Cards / Tokens / Otros

Respecto al tema de firma digital tenemos que implementarla y es fundamental para proteger datos, para que el ciudadano este valorado y no solo quedarnos en la firma digital; el concepto debe variar no podemos quedarnos solo en una tarjeta; porque pensar que el Banco Central lo va a poner todo en una tarjeta. Con los celulares de tercera generación los coreanos hacen e -Banking, toda la operación en el celular, porque el celular es una computadora, entonces porque no grabar la firma digital en el chip del celular en lugar de andar con un montón de aparatos.

Además está el certificado de conexión para validar de que sean sitios seguros y que puedan conectarse y el otro es el sellado a tiempo porque es necesario tener validez de que esos datos estén certificados y protegidos, también estos son conceptos que tenemos que validar.

Tecnología para educar

El programa se realiza a partir del re-uso tecnológico, el cual genera beneficios ambientales, económicos y educativos, por medio de estrategias que incluyen el reacondicionamiento, el ensamblaje, la tercerización, el mantenimiento, el acompañamiento educativo y la gestión de residuos electrónicos. Tenemos un programa de reciclaje, una empresa que nos asegura la eliminación de datos y

recuperamos esas computadoras para llevarlas a las escuelas que no tienen computadoras, solo hay 1200 escuelas conectadas de 9000 y esas 1200 solo cuentan con un solo laboratorio, es por eso que estamos ideando que las computadoras de las instituciones públicas y privadas sean donadas con ciertas características y vayan al centro de refraccionamiento, eliminar todos los datos, recuperar ciertos componentes y enviar las computadoras a las escuelas con mantenimiento y todo.

Al final de cuentas lo que nos falta es la aprobación del proyecto de ley de protección de datos, sentarnos a estructurar y revisar. Emitir lineamientos en la materia, no solamente la legislación sino que cada institución tenga todo un esquema y establecer estándares de intercambio de datos.

Finalmente la definición del ente que administre el tema; necesitamos definir quién va a dar las políticas, quién se va a encargar de la protección de datos y por supuesto capacitar a todo el personal que sea necesario.

Protección de datos en la Caja Costarricense del Seguro Social

Ana María Castro Molina

El tema a desarrollar hace un recorrido desde la definición de la unidad básica de información: "el dato", pasando por la articulación de los mismos en los sistemas de información y como los sistemas de gestión de la seguridad de la información vienen a proteger la misma haciendo uso de herramientas tecnológicas, mejores prácticas a nivel institucional orientadas al usuario, un pincelazo del estado actual de la capacitación a nivel nacional en el tema de la seguridad y la participación de este tema en las organizaciones, hasta detalles que parecen obvios pero que ponen en riesgo información sensible como lo es en el caso de el desecho o recicla de equipo tecnológico, todos estos temas desde un enfoque macro dada la asociación de los mismos a la protección de los datos. Se finaliza la ponencia con recomendaciones generales en procura de incentivar a quienes den lectura a esta documentación a tomar cartas en el asunto.

Pero para empezar lo primero que tenemos que saber es que es un dato: "es algún número, alguna palabra, algún concepto que por sí solo tiene un valor pero un valor muy general", así por ejemplo: podríamos tener el nombre María, el número 35 que por sí solos no dicen nada, podemos tener las siglas CA, un número que a simple vista

no nos dice nada como 102340897 y podemos tener la palabra terminar, así como una fecha por ejemplo 10/2/1974 para dar variedad al conjunto de datos que desintegrados no nos hacen sentido, pero que sin embargo con un mínimo grado de esfuerzo permite realizar una asociación de la cual podríamos concluir que: María cédula 1 02340897, fecha de nacimiento 10/2/1974 edad 35 años fue diagnosticada con cáncer estado terminal, entre otras interpretaciones que bien se pueden articular a la luz de la fuente de los datos, las condiciones en que se adquirieron, técnicas de ingeniería social, entre otras.

Entonces ¿por qué es importante saber que es un dato? Qué valor tiene? así como tener el conocimiento de ¿cuál es el tratamiento que hay que darle a los datos?. La respuesta es simple: Porque tenemos que saber qué es lo que vamos a proteger, para determinar cómo lo vamos a proteger.

Por lo general estos datos articulados son los que dan vida a los sistemas de información de nuestras instituciones, y en muchos de los casos se vuelven el activo mas importante de las mismas, de aquí se surjan mecanismos para darles la protección debida y es así como surgen los Sistemas de Gestión de la Seguridad de la Información, conocido por sus siglas SGSI, el cual constituye el "diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad, no repudio y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información".

Estos SGSI deben de ser por tanto el corazón de lo que llamamos seguridad informática, sobre la cual versa lamentablemente un falso paradigma: que corresponde a la falsa sensación de protección que da a la organización el contar con un software antivirus y un *firewall* lo cual es erróneamente llamado seguridad informática.

Pero realmente ¿Qué es la seguridad informática? La seguridad informática es una serie de componentes sistemas: software (SGSI, Antivirus, *Antispyware,* Scaneadores, entre muchos mas), *hardware* (IPS, filtradores, antispam, entre otros), etc. Que vienen a dar soporte y asidero a los siguientes pilares.

Disponibilidad de la información

No se puede seguir con el cuento de que uno va solicitar una información y que le dicen es que se cayó el sistema, no hay datos disponibles, por tanto tenemos que tener medidas de seguridad que nos den esa disponibilidad de la información mediante la aplicación de medidas de contingencia y continuidad del negocio, de forma tal que el usuario final no se vea afectado por posibles inconsistencias.

Adicionalmente nuestra información tiene que tener *confidencialidad*, dependiendo de la categorización que le demos y especialmente nuestra información personal la cual debe de tener un tratamiento especial. (Jurídicamente tenemos un vacío significativo en materia de la Ley de Protección de datos de las personas).

Por su parte, la *integridad* de la información es fundamental, ya que no se puede tener a medias, confusa, no coherente y menos inconsistente, cuando en su debido momento fue proporcionada de la forma correcta.

El *no repudio* que es otro de los pilares de la seguridad de la información, ya que no se puede alegar falsedad de la información a la que se tiene acceso si para tener acceso a la misma previamente el dueño de los datos tuvo obligatoriamente que facilitarlos, nadie puede decir esa información no es mía si yo mismo fui la persona que di esa información.

Identificar como se va a mantener porque efectivamente hay que estarlo actualizando y mejorando conforme avance la tecnología. Como vamos a verificar a implantar medidas que prevengan los ataques que se puedan dar en contra de la seguridad de la información.

Y desarrollar con base a la respuesta de los cuestionamientos anteriores un roadmap de los componentes que van a integrar el SGSI. Rápidamente una definición de cada uno de ellos como factores críticos de éxito en la protección de los datos, sobre todo por la constante evolución tecnológica a la cual nos vemos expuestos:

Seguridad lógica

Quienes tienen acceso a nuestros datos, como se accede a nuestra información, queda efectivamente un registro del acceso y manipulación de los mismos, quienes tienen acceso a esas bitácoras del movimiento de la información, son algunas de las aristas que deben de manejarse en este tema.

Normativa

Es lo que me respalda la gestión de los sistemas de seguridad de la información en sus respectivos niveles de publicación como políticas, normas, procedimientos, instructivos técnicos, entre otros y cada uno con su respectivo nivel de aprobación y comunicación a nivel institución, por ejemplo y en el mismo orden aprobación del más alto nivel institucional, mandos altos, mandos medios y nivel técnico.

El famoso antivirus

Gratuitos o licenciados que vienen a detener desde los virus más inofensivos como los joke / hoax (ej: Pac Man que se comía la pantalla y desaparecía con el movimiento del cursor) hasta los virus polimórficos que han evolucionado logrando inclusive el daño del hardware.

Seguridad física

Como tenemos acceso a los cuartos donde están los servidores, que registros se manejan, quien tiene acceso a los mismos, cuentan estos cuartos con las medidas recomendadas por el fabricante, entre muchas medidas que deben de ser aplicadas.

Filtrado de contenido

Qué filtro estamos aplicando sobre la información a la cual tienen acceso nuestros usuarios a nivel de endpoint, correo electrónico, navegación, mensajería instantánea, de forma bidireccional, de manera tal que la información que entra y la que sale no violente la protección de los datos sensibles.

Mejoras al esquema de autenticación con la incorporación del tema de firma digital, el cual si bien es cierto está dando sus primeros pasos a nivel país, ha sido exitoso en otras naciones en las cuales es indispensable para la identificación de las personas, los patronos y como control mediante el uso de las autoridades de sellado de tiempo.

Es necesario que las organizaciones apoyen el tema de la firma para dar un reforzamiento a los esquemas tradicionales de autenticación de usuario y password.

IDS/IPS

Herramientas tecnológicas conocidas como *IDS/IPS* los cuales se encargan sobre todo los segundos en la detección y prevención de intrusos a través de la configuración de firmas que van a filtrar el trafico anómalo que de forma bidireccional se mueva en la red, es así como este tipo de herramientas contribuyen a la protección de los datos, el costo de los mismos es elevado y la gestión para adquirirlos es compleja, mas el beneficio que aportan a la organización que hace uso adecuado de los mismos, retribuye toda la gestión asociada a poder contar con este tipo de dispositivos.

Antispam

Es otra de las herramientas importantes de destacar son las que vienen a depurar la información de pérdida de productividad y de alto riesgo que es enviada a los destinatarios de correo.

Adicionalmente existen metodologías y toda una base de conocimiento para la atención de incidentes mediante la aplicación de *medidas de contingencia y continuidad de la gestión*, mismas que deben de existir en cualquier organización.

Otro mecanismo indispensable es *la encripción* de la información sensible de forma tal que solo las personas que deben tener conocimiento de la misma puedan tener acceso de forma segura, existen múltiples algoritmos que dan soporte a este tema bajo modelos matemáticos complejos.

La jurisprudencia

Con que cuenta Costa Rica actualmente para dar atención a supuestos delitos informáticos es escasa y muy Light motivo por el cual las organizaciones deben de orientar esfuerzos a una mejora en este tema, retomando algunos de los principios de proyectos como el Habeas Data y promover la gestión de la Ley de Protección de Datos de las personas.

La ergonomía

Este tema de rara vez está asociado a la protección de los datos, sin embargo es necesario retomarlo en función de que las personas

que manejan información sensible las cuales están expuestas a sufrir lesiones de trabajo o enfermedades por no contar con las condiciones laborales y las posturas idóneas en su lugar de trabajo, lo cual incide en incapacidades y por ende muchas veces en un corte de la gestión de la información, resguardo de datos sensibles en equipos de estos funcionarios, entre otros que ponen en riesgo la integridad de la información.

La cultura informática

Es uno de los temas del SGSI que requiere de una mayor atención, ya que el usuario cuenta con algún conjunto de vicios aprendidos sobre el manejo de la información, apropiándose muchas veces de información que no les corresponde y es ahí donde debe de darse un proceso de desaprendizaje y adquisición de nuevos hábitos sobre el manejo de la misma, considerando las implicaciones del mal manejo de la información y las penas inherentes.

El análisis forense

Favorece el esclarecimiento de supuestos delitos informáticos y otros delitos, sin embargo el manejo de la evidencia debe de realizarse de forma tal que se maneja la cadena y custodia de la información, preservando la evidencia para ser utilizada en otras instancias superiores, es así que el buen manejo de la parte forensica es un factor de éxito delicado y que debe de ser tratado por especialistas en el tema.

Monitoreo de vulnerabilidades

Todos los días surgen miles de ellas y deben de existir los mecanismos para dar atención a las mismas, aplicando las contramedidas respectivas, lo cual implica un proceso constante de investigación.

Aplicación de estándares internacionales

En la gestión de la seguridad de la información, en el caos particular de la Caja Costarricense de Seguro Social, se da la aplicación de estándares como ISO 27001 en materia de seguridad informática, HL7 para el intercambio seguro de datos médicos; HIPAA que son unas regulaciones de los Estados Unidos sobre los expedientes médicos digitales, entre otros.

También nos regimos por lo que son los lineamientos y las normas que emite la contraloría General de la República. Adicionalmente de lo que es la normativa estamos trabajando con INTECO para traer normas internacionales y adaptarlas en la realidad costarricense, porque a veces la gente dice cómo vamos a implementar esto acá, si yo no sé de eso, no le vamos a decir a nadie que lleve el control de antivirus, como le vamos a dar esa responsabilidad si no sabe ni cómo hacer un password robusto.

Algunos Links de interés como la INTECO que adapta toda la normativa internacional a la necesidad de Costa Rica, el NFPA que es la parte de protección de incendios para todo lo que son centros de cómputo:

- www.inteco.or.cr/
- www.nfpa.org/
- www.ieee.org/

Reciclaje…y la información

El tema del reciclaje y la información, nos hemos preguntando a donde van a dar los residuos electrónicos y sobre todo donde van a dar los datos que estaban dentro de estos componentes tecnológicos que desechamos?

Damos un equipo de baja y digamos que por el mejor procedimiento llamamos a una empresa que de forma sostenible se deshaga de los desechos que no contamine el ambiente, pero cuáles son los procedimientos de desechos de la información, se destruyen las cintas, como hacemos para destruir los discos duros, porque a veces decimos es que ya no sirve ni siquiera prende y cuando llega a manos de un especialista logra restaurar la información. Entonces un llamado a la conciencia ambientalista y en cuanto al desecho de esos datos, en la basura hay quienes se pueden aprovechar de eso.

Nosotros trabajamos con una empresa que se llama la Bodeguita, debido a que fue la única que no nos cobró por nuestra basura electrónica, ya que el resto de las empresas cobran alrededor de un dólar por cada kilo de basura, cobrando por la basura a desechar de la cual ellos obtienen un beneficio económico y adicionalmente cobrando el transporte de los desechos.

Esta empresa adicionalmente emite un certificado sobre el material reciclaje en conformidad con la protección del medio ambiente cumpliendo con lo establecido en la normativa de ISO 27001, la empresa asume la responsabilidad sobre el manejo de los residuos y para tales efectos tienen nexos internacionales ya que por ejemplo: los monitores son altamente contaminantes y no existe en el país tecnología para su proceso motivo por el cual deben de ser tratados en planta especiales fuera de Costa Rica.

¿Por qué es importante tocar el tema del reciclaje? Además de la preservación y desecho correcto de la información, porque ninguno quiere estar buscando sobrevivir en un mundo lleno de basura tecnológica y con un medio ambiente altamente contaminado por no tomar las medidas respectivas a tiempo.

Y otros componentes que se vayan agregando al SGSI de cada institución conforme evoluciona la tecnología y se profesionalizan los ataques, dentro de los cuales es importante destacar.

Elspyware

Que como bien se traduce es un software espía el cual de forma silenciosa esta obteniendo información de la estación de trabajo del usuario.

Una de las nuevas tendencias es el *Smishing*, en el cual mediante publicidad o ingeniería social se envían mensajes al móvil personal alegando la obtención de premios, ringtones gratuitos, links a sitios de nuestro interés, los cuales son potencialmente peligros de ser accesados, y que por lo general roban información sigilosamente de la libreta de contactos del celular, introducen virus, etc.De igual forma el *Vhishing* en la telefonía VOIP.

La suplantación o spoofing

Que ahora actúa de forma digital, por ejemplo de forma análoga a la situación que se ha presentado en algunas dependencias de salud donde ante la carencia de un mecanismo robusto de identificación de clientes hospitalarios, personas fallecidas han ido a solicitar citas de atención, ante la posesión de documentos de estos por personas que pagan por ellos o que simplemente los sustraen para obtener el beneficio.

La suplantación a nivel del DNS

Cuando se apropian de la información de este para suplantar los nombres de dominio, generando dominios falsos, donde el usuario cree que está ingresando al sitio habitual, sin embargo lo está haciendo a un lugar falso en el cual deposita datos clave como lo son información de usuario / contraseña / cuentas bancarias / etc.

Spam

Es todo el famoso correo basura que llega, muchas veces como resultado de el *trashing* que efectúan los ciberdives al analizar los hábitos de navegación del usuario, identificando así los interés del mismo.

SQL inyection

Cuando se inyecta código a las aplicaciones, que es código infectado y se sustrae información.

Keyloggers

Registran cualquier carácter que se digite por teclado y que va quedando en una bitácora local o es enviado por ftp/correo electrónico sin conocimiento del usuario.

Y una de las técnicas que se están utilizando mucho que es la *estenografía,* identificado a nivel domestico ya que los muchachos estaban vulnerando el control de padres al no chatear por texto sino por imágenes, ya que estas ocultan texto, aplicaciones, entre otros. De igual forma y análogo a una manera tan sencilla como mandar una imagen también hay atacantes que lo que hacen es mandar bombas lógicas que lo que explotan es código y lo que hacen es sustraer información, es una realidad y esta pasando ya dista del CSI.

Y tal vez de todos estos ataques y problemas de seguridad el más grave y el menos controlable es el famoso usuario, porque el usuario es muy tranquilo y muy falto de cultura informática, al usuario no le importa tener una contraseña en blanco o fácil 1, 2, 3 o passwords simples de recordar, entre otros muchos males usuarios, en el tema de la contraseña lo que pasa tampoco existe la cultura para enseñarle al usuario a hacer una contraseña robusta.

¿Cómo hacer una contraseña robusta? Pues muy fácil a mi me gusta una canción tal vez esta de los Simpson "sonó, sonó, sonó, te llaman del bar de Moe" entonces lo que hago es tomar la primera letra de cada una de las palabras de la frase, obteniendo una contraseña ssstldbdm la cual puede incorporar letras mayúsculas o números, lo cual va a darle robustez y el usuario siempre lo va a recordar, como por ejemplo: S3tldbdm05.

Mas no logramos nada si el usuario continua haciendo un montón de post-it con las contraseñas las cuales pega o pone en su equipo, sobre de escritorio, etc; le da su usuario y contraseña a otro compañero para que le haga el favorcito, da sus datos por teléfono, entre otras, la cuales son malas prácticas deben de eliminarse.

Otro vicio del usuario es que con cualquier cosa que ve Internet gratis o de promociones da sus datos personales y entra a sitios con exploits que pone en riesgo no solo su información personal sino también la información que transita por la red si su equipo está conectado a la misma o en algún momento se conecta.

Por tanto es urgente enseñar al usuario sobre el uso correcto de la información, así como la responsabilidad que tienen al manejar la misma, en procura de disminuir los incidentes de vulneración y mejorar los esquemas de seguridad.

Situación actual de la seguridad informática a nivel nacional

El país carece de programas académicos que formen profesionales en el tema de la Seguridad Informática, de ahí un llamado a la magna UCR para que se promueva la creación de los mismos y se facilite la explotación de esta temática a nivel educativo de cara a las necesidades del país y el creciente riesgo de perdida, trasiego, alteración y otras tipificaciones de delitos informáticos que pueden versar sobre la información sensible que manejan las organizaciones.

A nivel institucional, la creación de dependencias que atiendan el tema de la Seguridad es incipiente, salvo el caso de las entidades bancarias que han apostado a este tema desde hace mucho tiempo atrás y cuentan con implementaciones de SGSI interesantes y con distintos niveles de madurez, sin embargo a nivel de otras instituciones

publica, el tema esta apenas tomando fuerza y lamentablemente bajo un error de organigrama es ubicado dentro del área de las Tecnologías de la Información y Comunicaciones, siendo juez y parte en muchas de las actuaciones que llevan a cabo, las mejores practicas documentadas a nivel europeo sugieren que esta nueva rama de la organización forme parte de una Gerencia de Riesgo la cual este directamente ligada a los mando superiores de las instituciones de forma tal que su cobertura no se vea limitada por su ubicación, ni sea coaccionada por el nivel de dependencia.

Acciones sugeridas

A titulo muy personal estas son algunas acciones sugeridas en cuanto al tema de protección de datos o que tenemos que hacer en cuanto al tema de proteger nuestra información.

Lo primero es romper paradigmas, aquí me quiero poner un poquito en desacuerdo con lo que vimos en las jornadas de Cyber seguridad alguien pregunto si se podía llevar un curso de hacker y le dijeron no, como se le ocurre, pero yo les pregunto ¿las personas que trabajan para combatir los hackers, no deberían saber lo que saben los hackers? Yo creó que uno debería tener igual o más formación que un hacker para saber cómo te están atacando, como detenerlo, por donde me están atacando, para poder atender este ataque, entonces romper esos paradigmas.

Educar y responsabilizar al usuario, creando una cultura de seguridad de la información, esto desde la edad escolar que empiecen a responsabilizarse de la información.

Establecer dependencias de seguridad informáticas capacitadas, se que no es una figura muy común en las instituciones y que hay muy pocas y que se están empezando apenas a implementar, esto a pesar de lo indicado anteriormente sobre el sector bancario, pero es necesario que se implementen las áreas de seguridad en las empresas y es necesario que la gente que está ahí este capacitada para que sepa en qué es lo que está trabajando.

Implantar políticas integrales de seguridad alineadas a la lógica del negocio, con base en una visión global de la institución, análogo a

un bosque donde no solo vamos a observar algunos árboles sino vamos a abstraernos y observarlo en toda su magnitud y desde todas las aristas posibles.

Muy importante que las universidades formen especialistas en seguridad a nivel nacional, y que se promueva el reconocimiento de estudios obtenidos en el extranjero haciendo uso de los recursos universitarios y criterios de universidades como la UCR, UNA y TEC, dejando de justificar el no reconocimiento por normativas que datan de 8 a 10 años de antigüedad.

Se debe de cambiar el pensamiento de formación académica promoviendo la formación virtual sobre todo en temas tan de de punta como lo es la seguridad, donde diariamente se cuenta con un nuevo tema por aprender.

Reforzar la legislación de temas que son así como para ayer el tema de protección de datos personales, la detección de delitos informáticos que si bien ya hay una institución que está trabajando en detener estas actividades, que no sean solo tres artículos generalísimos que haya una legislación en general que trate el tema de los delitos informáticos, porque los delitos se van profesionalizando y no hay jurisprudencia para penalizarlos el delito queda impune.

El usuario debe de responsabilizarse de la información que manipula y velar por que sus datos personales no corran el riesgo de ser mal utilizados.

Protección de datos en el Banco Nacional

Cilliam Cuadra Chavarría

Esta presentación intentará compartir la experiencia en la protección de datos en el Banco Nacional identificando factores claves de éxito en el proceso que permitió consolidar un grupo formal para la seguridad de la información, lo cual no se hace de la noche a la mañana. En este camino se han tenido muchas experiencias, se ha debido renovar, actualizar y aprender todos los días; porque todos los días debemos aprender cosas nuevas especialmente en los bancos que representan siempre un objetivo interesante al ser responsables de recursos económicos.

Esta situación de "objetivo interesante" se explica por el auge del dinero electrónico. Es posible que todos los presentes hayan tenido la oportunidad de ingresar a la página electrónica de su banco para hacer uso de las herramientas de banca electrónica y es posible que los que hacen uso de esta modalidad de servicio utilicen más dinero electrónico que lo que utiliza en forma de efectivo; esto ya es normal para cualquiera que haya cumplido más de 18 años (alcanzando la mayoría de edad) en Costa Rica.

Aprovechando la invitación del PROSIC a estas jornadas de reflexión deseamos poder colaborarles con la idea de que la seguridad

de la información es un proceso continuo que requiere el apoyo decidido de la administración. Optar por seguridad de la información es decir sí a un proceso, no a una iniciativa que arranca un día y que cuente solo con una fuerte emoción durante los primeros años, tiene que ser una decisión constante de la gerencia.

Reseña histórica

En el Banco Nacional se inicia en 1998 con una pequeña unidad dedicada a la atención de los procedimientos y normas de seguridad. El Banco Nacional entendió desde el principio que para tener seguridad el primer paso era tener una política de seguridad, en ese tiempo no estaban los avances a nivel internacional en materia de seguridad pero ya existían iniciativas sólidas para documentar este aspecto trascendental en el proceso.

Dentro de las funciones generales asignadas en su momento se tienen

- Planificar, proponer, controlar y apoyar en la ejecución de normas y procedimientos de seguridad informática.
- Proponer y desarrollar sistemas de seguridad informática para el desempeño de las funciones tecnológicas especializadas.
- Vigilar el desarrollo de las normas y procedimientos de seguridad informática aprobadas.
- Asesorar y participar cuando corresponda, en la implantación de las normas de seguridad informática.
- Coordinar el desarrollo del Plan de Contingencia de Tecnología Informática.
- Apoyar las labores de auditoría de sistemas de información del Banco.

Este proceso inicia entonces con un programa principal para establecer políticas, procedimientos, y estándares de seguridad; para esos años el concepto de política de seguridad no tenía mucha madurez. Ahora a lo largo de las Jornadas han podido constatar como los expositores pueden expresarse sobre políticas de seguridad con mucha propiedad. En el banco se ha tenido que recorrer todo ese camino de madurez en este proceso.

Como base para la Política de Seguridad se inició con el Orange Book del departamento de Defensa de los Estados Unidos dado que era el documento estructurado más reconocido sobre el tema. Este documento al igual que sus herederos vigentes actualmente tiene la característica de que indica de forma precisa lo que debe hacerse en las instituciones, este es un estilo basado en la cultura militar americana, lo cual lo hace muy detallado y difícil de digerir por el usuario latinoamericano.

Otros de los avances iniciales fueron:

- Creación del Comité de Estándares de Tecnología.
- Implementación de centro de respaldos alterno de medios magnéticos.
- Elaboración del primer Esquema de Seguridad Informática Institucional.
- Evaluaciones de seguridad en agencias y sucursales.
- Elaboración de los primeros Estándares de Control de Calidad para Desarrollo de Sistemas.
- Elaboración del primer Plan de Contingencia de la DCTI.
- Elaboración de la Guía de Planes de Contingencia para el Proyecto Año 2000.

La creación del comité de estándares permitió avanzar en materia de estándares definiendo aspectos básicos en el área de desarrollo de aplicaciones y compra de equipos. El centro de respaldos alternos elevó el nivel de preparación para eventos no deseados y permitió un adelantamiento a las normativas que posteriormente los reguladores adoptarían.

1998-2000

- Establecimiento del Manual de Seguridad Informática, basado en el Orange Book del Departamento de Defensa de USA.
- Creación del Comité de Estándares de Tecnología.
- Implementación de centro de respaldos alterno de medios magnéticos.
- Elaboración del primer Esquema de Seguridad Informática Institucional.

- Evaluaciones de seguridad en agencias y sucursales.
- Elaboración de los primeros Estándares de Control de Calidad para Desarrollo de Sistemas.
- Elaboración del primer Plan de Contingencia de la DCTI.
- Elaboración de la Guía de Planes de Contingencia para el Proyecto Año 2000.

Se realizó todo un trabajo de promoción porque para hacer un cambio cultural en una institución estatal grande en un momento muy efervescente al existir cambios en nuevas gerencias e integración de ideas muy innovadoras que hoy hacen muy diferente el Banco Nacional.

En medio de ese ambiente parece siempre difícil lograr la prioridad de ideas y atención de algo tan nuevo porque para el año 1999 – 2000, el idioma de seguridad no calaba en el personal o el país. Hablar de tecnologías seguras, tenía su complicación, mencionar el tema de amenazas de seguridad informática tenía su complejidad, la brecha tecnológica y en particular el acceso a Internet jugaban un papel trascendental para que el mensaje no fuera tan permeable. Con el nivel de acceso a Internet y la actual reducción de la brecha tecnológica se forma y comparte más conocimiento alrededor de las redes.

Sin embargo, toda la atención de los medios e incluso gubernamental sobre lo que se denominó el Problema del Año 2000, permitió integrar estas iniciativas en la corriente de prioridad. Esta misma fue la forma en muchas empresas a nivel internacional lograron la atención sobre aspectos de la administración de la información y en particular sobre su seguridad.

Aprovechando la coyuntura de la situación relacionada con el tema mencionado del Año 2000, se actualizan las guías para la atención de emergencias en caso de terremoto, incendio o inundación, orientadas a las oficinas regionales, incorporando el tema tecnológico de modo que los funcionarios tuviesen conciencia de que el equipo y la información son parte fundamental de lo que debe protegerse aún en circunstancias difíciles.

Del mismo modo, la exposición de atención sobre el tema Año 2000, permitió elaborar un trabajo en temas de normativas de seguridad en

redes y telecomunicaciones, en planes de contingencia en centros de cómputo, se elaboró una normativa de usos de Internet, de Intranet y de correo electrónico con miras de que la totalidad de los funcionarios tuviesen acceso a Internet y reducir la brecha tecnológica interna. Estos aspectos contaron con la ventaja de que la gente ya sabía cuáles eran los procedimientos seguros y políticas de seguridad.

Uno de los aspectos relevantes de estos tres años iniciales fue la integración de las primeras herramientas de seguridad de la era de las comunicaciones e interconexión de redes como los antivirus, el primer *firewall* y los primeros detectores de intrusos. De esta forma se contó con una infraestructura ordenada y segura para la operación de un servicio interno de correo electrónico y acceso a Internet. A la vez que se preparó la organización para integrarse a los servicios de banca electrónica que luego nos permitirían estar a la vanguardia.

En el tema de ser pionero en seguridad informática el Banco Nacional ha experimentado situaciones interesantes, por ejemplo al ingresar el primer *firewall* se determinó que no se había traído un *firewall* al país (al menos utilizando la infraestructura de aduanas normal) al punto de que tuvimos documentar en detalle que hacía la "caja" para que se crearan las estructuras necesarias en los catálogos que permitiese diferenciar la funcionalidad. Recientemente, algo parecido nos pasó con los *tokens* de autenticación, en las aduanas no tenían documentación al respecto dado que nadie había traído esos aparatos por la vía normal de importación.

Finalmente avanzamos en la estructuración de oportunidades de capacitación formando parte de la iniciativa de la ACM (Association for Computing Machinery) de dedicar un día anual al tema de la seguridad de la información con la Celebración del Día Internacional de la Seguridad Informática en su primera edición. Esta celebración se realiza el 30 de Noviembre de cada año a nivel internacional por lo que aprovechamos impartir charlas con presentaciones de expertos internacionales en el tema de la seguridad de la información.

2001-2004

- Revisión Integral de Efectos Año 2000.
- Inicio de la campaña para la Identificación y Disminución de Riesgos Informáticos.

- Implementación de la primera infraestructura de seguridad para servicios de correo electrónico y navegación en Internet.
- Elaboración de la guía para realizar análisis de continuidad del negocio.
- Inicio de la labor de monitoreo integral de la seguridad.
- Implementación del ISRT (equipo de respuesta ante incidentes).
- Implementación de controles especializados Anti-X en el perímetro y navegación en Internet.

Se realiza una revisión integral de efectos del año 2000, mejorando los controles y se avanza en la búsqueda de una administración sostenible de la seguridad informática mediante la identificación y clasificación de riesgos informáticos lo que concluye con un diseño de una estructura de riesgo que ha sido premiada a nivel internacional dentro del banco.

Se implementa una infraestructura de seguridad en correo electrónico y navegación en Internet que para ese tiempo ya integró el monitoreo, que no era una cosa muy frecuente en el país. Este monitoreo le permitía al Banco Nacional establecer niveles de alerta. En esta experiencia se logró identificar temporadas de alto riesgo relacionadas con el interés de estudiantes colegiales que en sus vacaciones deseaban probar y mostrar sus nuevas habilidades informáticas. El interés por el "juego" con herramientas de seguridad llegó implicar que las vacaciones en Costa Rica tomaron tanta importancia como las vacaciones de verano de Estados Unidos.

Con la capacidad de recordar que provee la información electrónica, el banco ya empezó a tener información de lo que realmente pasa en Costa Rica en el Internet, esta información tiene mucho valor dentro de este proceso que ha llevado el Banco Nacional. El valor de la información se basa la posibilidad de identificar variables del entorno de la Internet de Costa Rica como la existencia de *software pirata*, el nivel de actualización de los equipos, la distribución geográfica de los usuarios, etc. Dentro de este proceso se logró madurar el concepto de monitoreo hasta llevarlo a la conformación del equipo de respuestas a incidentes.

Con un equipo más maduro de trabajo se consolidan las iniciativas para una arquitectura del sistema de seguridad informática, en eso se construye el conocimiento de las áreas que deben ser consideradas para controles y riesgos que se puedan dar. Este proceso se lleva a cabo en varias etapas, iniciando con un análisis que permita dimensionar cuál es el alcance de las aplicaciones existentes y en desarrollo, redes, interconexiones y base de datos que tienen las empresas. Posteriormente se aplica el modelo de riesgo definido para identificar las amenazas y se establecen los controles que permitan un balance entre el costo del control y su efecto en caso de materializarse la amenaza. Para esto se utilizan esquemas de retorno de la inversión que permitan mostrar a la administración el equilibrio financiero asociado al control. El dominio del retorno de la inversión que es un tema importante que se debe rescatar porque permite un lenguaje entre la administración y los técnicos y refleja finalmente un equilibrio entre la inversión que se va hacer y lo que vamos a proteger.

El banco incursiona en la banca por Internet, lo que genera un esfuerzo para el establecimiento de los controles y mejores prácticas de primer nivel. En cuanto a la banca personal si bien el banco no fue el primero en brindarla, si fue muy importante para la administración que el producto cumpliera con los parámetros adecuados de seguridad. Esta visión de la administración permitió posicionar la banca por Internet en un nivel de liderazgo regional no solo en cantidad de usuarios sino en montos transados.

Buscando un paralelo, es conocido que grandes empresas líderes hoy como eBay y Amazon no necesariamente fueron las primeras en desplegar el concepto de negocio que las hace famosas, pero lo hicieron de forma tal que fueron capaces de crecer más que ninguna otra en su ramo por sus procedimientos y garantía de seguridad en las transacciones.

La recomendación que surge para los que están desplegando iniciativas en Internet es que la seguridad de información sea considerada dentro del ciclo mismo del producto que ofrecerán, de esta forma sus expectativas de crecimiento y retorno de la inversión ya incluirán los factores de costos asociados a los controles que sea necesario establecer.

Una de las iniciativas que más ha pesado en el éxito ha sido el inicio temprano del despliegue generalizado de la plataforma de control de contenido. Se inició con la seguridad perimetral mediante el despliegue de la plataforma Anti-X. El Anti-X se refiere a la protección *anti-virus, anti-spam, anti-spyware y anti-malware.*

Esta iniciativa ha permitido que en tanto en cualquier empresa nacional interconectada a Internet se reciben entre 3 y 12 correos *spam* o no deseados en el día, en el Banco Nacional los funcionarios no perciben el *spam* como una amenaza dado que no lo han experimentado gracias a los controles. La experiencia de clientes de grandes proveedores de servicios de correo como Yahoo o en Hotmail donde se utilizan hasta 7 niveles de filtros especializados es que se reciben alrededor de 20 correos basura por día. El inicio temprano permitió afinar los controles de contenido de modo que su operación no entorpezca el servicio y permita la protección requerida. La recomendación es que las empresas identifiquen sus necesidades de protección y las implementen en conjunto con un producto. De esta forma el producto será más valorado por los usuarios y el costo de atención de usuarios por aspectos ocasionados por el control será menor.

En el tema de certificados digitales convertimos al BNCR en el primer banco que completó una implementación que habilitó la firma digital en los correos internos. La limitación de esta iniciativa se centró en que no se contaba con una legislación que respaldará para llevarla al nivel del cliente. Sin embargo, los beneficios internos de este trabajo permitieron reducir los costos en el manejo de papelería.

Para el año 2003 se designa un equipo de trabajo que permitió elaborar una política de seguridad informática basada en ISO 17799 (esta especificación actualmente es parte de la familia ISO 27000). Las políticas basadas ISO tienen la ventaja de permitir el desarrollo de los controles a partir de objetivos de control. Para cada empresa puede ser distinta la respuesta de control al objetivo de control, dependiendo de la necesidad en esa área específica, el presupuesto, y el resultado del análisis de riego. La recomendación es que todas las empresas pueden hacer uso de la recientemente renombrada familia ISO 27000 en un banco o en cualquier otra institución para el desarrollo de su política de seguridad.

Este paso implicó una evolución y revisión en el diseño de normativas para el desarrollo de aplicaciones, acceso a redes y bases de datos. Se revisó la implementación de la arquitectura de la información y la seguridad, para ubicar los aspectos que con la nueva política era necesario normar más allá de un modelo.

Uno de los errores básicos que se comenten en las organizaciones es que define una estrategia de seguridad y no se revisa constantemente para identificar si continua alineada al negocio especialmente cuando el crecimiento de la organización se ha presentado. La recomendación es que no piensen que ya tienen su sistema de seguridad definido para un momento en el tiempo de la organización y que con eso les va a alcanzar para el crecimiento, eso se ha evitado en el Banco Nacional. Como parte de esa visión, actualmente se están incluyendo las ideas de control y estructuras que permitan dar un salto de "administración de la seguridad de información" al "gobierno de la seguridad de información" con la ayuda de organizaciones internacionales sobre todo ISACA.

2005-2007

- Implementación de certificados digitales en diversas aplicaciones y autenticación remota.
- Análisis forense sobre incidentes institucionales.
- Zonificación de la Red Institucional e implementación de controles relacionados.
- Diseño de normativa para los esquemas de seguridad para bases de datos.
- Implementación del Modelo de Encripción.

Dentro de los temas que abarca la seguridad de la información se priorizó la normativa de seguridad en bases de datos para brindar un marco común de referencia que permitiera el crecimiento estimado en los múltiples canales que tiene la organización.

Paralelamente se desarrolla el Modelo de Encripción que permite un lenguaje común entre desarrolladores de aplicaciones y administradores de redes, este modelo está alineado con la iniciativa de zonificación de redes con la finalidad de alcanzar la adecuada

protección de la información en tránsito y almacenamiento que se persigue con la encripción de datos.

En esta etapa de nuestro proceso se desarrolló un completo análisis de zonificación de la red. De esta forma se estableció un mayor nivel de granularidad en cuanto las diferentes capas de protección y las actividades permitidas en cada segmento específico. La recomendación general es que las organizaciones busquen en un proceso de segmentación y zonificación de redes el equilibrio necesario para que los usuarios tengan la sensación de trabajar con comodidad en su segmento asignado el cual le estará disponible basado en su necesidad de acceso y su necesidad de saber.

Con un detalle de la zonificación deseada, el crecimiento del ancho de banda que permitió el desarrollo en Internet nacional y haciendo uso de la ventaja de contar con una Infraestructura de PKI interna, se habilitó algunos servicios a lo interno de tecnología como el soporte y monitoreo remoto; logrando una de las primera iniciativas reales de teletrabajo en ejecución en el territorio nacional.

Finalmente, en esta etapa del proceso se busca la especialización del equipo en actividades de trascendencia en procesos de investigación como el análisis forense. Para lo cual se adquieren herramientas de integración y administración de bitácoras. Internamente se realizan procesos fuertes de estandarización de registros de auditoría en las aplicaciones buscando alcanzar al máximo la trazabilidad de las transacciones. La recomendación que surge es que las empresas realizan un análisis de sus registros de auditoría en todos los niveles aplicativos, desde el proceso mismo de identificación y autenticación del usuario en la red hasta la aplicación de las modificaciones que sugieren los comandos disponibles a los usuarios, de esta forma que puedan reconstruir la transacción a partir del principio de atomicidad.

2007-2009

- Enmarcado en el Proyecto Cumbre se inician las campañas *AntiPhishing* con la finalidad de alertar a los clientes sobre esta amenaza y la inclusión permanente de controles relacionados.
- Implementación de certificados digitales en los servicios que ofrece el Banco a sus clientes incluyendo Oficina Virtual.

- Implementación del Proyecto BN Identidad Virtual basado en OATH.
- Participación en foros y conferencias nacionales e internacionales concientizando sobre las amenazas y controles en el ámbito financiero.
- Celebración del Día Internacional de la Seguridad Informática –Año 10.
- Integración de nuevas herramientas en la vida electrónica de los clientes.

A partir de la identificación de amenazas crecientes en el campo financiero se inicia con las primeras campañas *Anti-Phishing* resaltando el hecho de se inicia antes de que en Costa Rica sucediera el primer caso de *Phishing*. Las encuestas realizadas mostraron que los usuarios pensaban que a quién le pasaba una de estas situaciones de *Phishing* era porque no tenía suficiente información o suficiente entendimiento de lo que representa Internet. La realidad fue otra y como se ha mostrado los usuarios son víctimas de *Phishing* porque muestran una conducta muy distinta a la que presentan en el mundo físico. La confianza juega un papel trascendental, el banco a través de la campaña busca cambiar este panorama cultural. Algo para rescatar es que en Costa Rica no es tan grave la situación de *Phishing* como la prensa lo hace ver, todavía no nos vemos tan afectados por esto como otros países y es muy posible que no continuemos a partir del cambio de estrategia que han asumido los bancos y los clientes en torno a la seguridad y su costo.

Por ejemplo, en Brasil los bancos grandes aún hoy se reciben 2000 quejas por día de personas víctimas de fraudes relacionados con el robo de identidad. En Estados Unidos, por su parte, el problema implica cifras de hasta 100 millones de dólares por día, alcanzando el 1% de la población. En Costa Rica ha llegado a alcanzar al 0.02% de la población lo cual está es muy por debajo de lo que ha pasado en Inglaterra, Argentina, Chile o España. Desde el punto de vista noticioso se muestra una situación más crítica de la que permiten ver las estadísticas.

Aprovechando la madurez alcanzada en el acceso remoto seguro se dispone de las tecnologías para el uso de cara al negocio con

la iniciativa conocida como Oficina Virtual, proyecto que ha logrado importante premios en el ámbito financiero en Latinoamérica al permitir que un gestor de negocios pueda estar en cualquier parte del país y tener acceso al banco en forma segura. El alcance ha permitido compartir la experiencia con empresas transnacionales clientes del banco para colaborarles en iniciativas similares en el campo de las ventas.

Recientemente se ha desarrollado el proyecto denominado Identidad virtual sobre el cual se desplegado una importante campaña. Este proyecto tiene dentro de sus características que utiliza tecnología de administración de autenticación basada en OATH, el cual es un protocolo abierto. Al ser un protocolo abierto múltiples proveedores y desarrolladores participan en un foro internacional donde se definen las reglas que lo soportan. Todos pueden desarrollar tecnologías basadas en sus algoritmos y estructuras. Esta tecnología posee la ventaja de que cualquier mejora que se desarrolle en el área de autenticación puede ser incorporada con facilidad. Desde el punto de vista del cliente nos prepara para poder brindar múltiples modelos de autenticación; así si un cliente prefiere un certificado digital porque se siente más confortable podemos suplirle la tecnología, si quiere un *token OTP* le podemos facilitar uno. De la misma forma se protege el ingreso de las claves con el Teclado Virtual dado que se ha determinado que el uso de *software* tipo *malware* y tecnologías tipo *"keyloggers"* son dos de las técnicas utilizadas en el medio para el robo de identidad.

El teclado virtual se convierte, adicionalmente, en una respuesta al uso de *software* no licenciado en Costa Rica, la cual es una de las amenazas más fuertes que se enfrentan. La tecnología del teclado virtual del Banco Nacional crea una burbuja de seguridad en la memoria del computador donde se ejecuta de modo que otras aplicaciones que se ejecutan en conjunto no tienen acceso a los datos que se están procesando, de este modo se aísla el efecto de *software malicioso* que pretenda compilar la información confidencial de los clientes. El *software malicioso* se aprovecha de la gran cantidad de equipos que no pueden utilizar las actualizaciones de seguridad que generan los proveedores, los cuales las limitan a las estaciones que

puedan demostrar la integridad de su licencia. La razón más común para no poder actualizar es el uso de *software pirata* en Costa Rica; hay una altísima proporción de la población que tiene un *software pirata*, esto a pesar de que está generando más conciencia y se discute con más interés el tema de seguridad. El *software pirata* es una barrera de cara al cliente y esta es una respuesta efectiva para lidiarla.

Este paso en la protección de la identidad y de la información ha sido un éxito porque hay tecnologías innovadoras que soportan lo que es visible para el cliente. Otros bancos en el área de Centroamérica han seguido la idea de implementación del BNCR, en este momento hay 5 bancos a nivel de Centroamérica estudiando o implementando sus soluciones al tema de autenticación y robo de identidad con las mismas tecnologías abiertas utilizadas en el BNCR.

En cuanto a la organización y su evolución la fase actual muestra definición de 5 procesos definidos como: Administración de la Seguridad, Seguridad en Infraestructura, Desarrollo de Normativa, Validación y Verificación y Respuesta a Incidentes.

Este es un cambio que está en el ámbito internacional sobre el cual se ha trabajado para adaptarlo y se está en la etapa final de afinamiento. Es posible que este se torne un año difícil en tanto se afinan estos detalles, pero el cambio ya inició con la creación de las diferentes áreas. Con esto se tendrá una organización lo que se denomina gobierno de la seguridad de información.

En este modelo de trabajo adoptado siguen siendo importantes las prácticas de ejecución de autoevaluaciones de riesgo; capacitación y concientización en aspectos de seguridad de la información; seguimiento y monitoreo a la proliferación de virus, *malware y Phishing* a nivel internacional; participación en proyectos para mejorar la arquitectura de seguridad; la atención de incidentes de seguridad y la actualización y desarrollo permanente de las políticas y normativas en seguridad.

Como parte del proceso de concientización se busca implementar ideas que sean constantemente innovadoras; por ejemplo, utilizamos *"gadgets"* que le recuerden a los colaboradores el tema de la seguridad de la información donde quiera que estén. Recomendamos el

uso de estas técnicas para lograr un despliegue efectivo sobretodo par aquellas empresas que estén creando un grupo de seguridad de la información. Esto les permitirá visibilidad con la consecuente ventajas de que los colaboradores tendrán presente que tiene a quien recurrir para reportarle los incidentes. Estas prácticas identifican la función dentro de la organización. El tema de costos debe ser valorado dentro del esquema de riesgo y retorno de inversión que se haya definido.

Entretanto, ¿qué estamos viendo como amenazas que vamos a enfrentar estos días?. Particularmente el hecho de que los usuarios siguen ingresando a Internet desde estaciones e instalaciones de Internet no seguras; los usuarios utilizan redes inalámbricas con total confianza sin importar si son seguras o si el proveedor de la red es confiable; la proliferación de Internet Café´s ha permitido una importante reducción de la brecha tecnológica pero incrementa la posibilidad de instalaciones "fantasma" que únicamente persiguen el robo de identidades.

Como organización con servicios en Internet no esperamos que los usuarios lo sepan todo pero lo que necesitamos y enfocamos en las campañas es que las amenazas son reales. Se busca incentivar la malicia de saber cómo se conectan, de donde se conectan, que el banco tiene un sitio de Internet que mejora su calidad de vida, pero la responsabilidad por la seguridad es de todos.

Otro de los aspectos que nos ocupan es dejar de lado las claves como único factor de autenticación, se está trabajando con los dispositivos del proyecto Identidad Virtual y con la firma digital.

En cuanto a la firma digital estamos buscando medios para dotarle los factores de usabilidad y portabilidad a esta tecnología, nada hacemos con toda la tecnología de firma digital y toda la infraestructura que se ha creado si no se eliminan las barreras que siguen impidiendo el despegue de esta tecnología en los últimos 25 años. Hasta hoy el usuario normal no tiene confianza en la firma digital y su nivel de portabilidad y costo dista mucho de los requerimientos y disponibilidad de Internet.

La barrera de portabilidad en este caso implica que se tendrá que enfrentar a la necesidad de instalar *"drivers"* en cada máquina donde se desee utilizar la tecnología, hay que instalar lectores de tarjetas, esto

es complicadísimo para el 60% de la población y más si consideramos que el proceso requiere derechos exclusivos de los administradores lo cual en las empresas es parte de los controles que más éxito han tenido. Con respecto al costo se debe reducir de modo que esta tecnología no se convierta en un factor que contribuya al incremento de la brecha tecnológica.

En el campo del fraude se enfrenta desarrollos de *malware financiero* más sofisticado, hoy día hay *malware* creado para engañar a un cliente que utiliza certificados digitales. En Inglaterra se enfrenta una dualidad en los tribunales porque se estableció una garantía para las organizaciones financieras al incorporar los certificados digitales y firma digital, pero el cliente indica que no realizó las transacciones que reclama, no tiene la culpa de la existencia de este tipo de *malware* y los bancos se niegan a pagar porque el cliente tiene un certificado digital esto va a cambiar los paradigmas en los próximos años.

Finalmente, estaremos pendiente de la movilidad de los clientes. Este tema interesa porque hoy en día los más jóvenes utilizan muchas aplicaciones y tecnologías portables, el estudiante promedio universitario lleva consigo todo en *software* que requiere de forma portable en un disco externo o en llaves mayas de gran capacidad. Estas tecnologías se convierten en una oportunidad excelente para el desarrollo y propagación de *malware* y problemas adicionales para los que hay que implementar controles y generar cultura.

Protección de datos en el Poder Judicial

Rafael Ramírez López

Los avances tecnológicos experimentados por la sociedad en los años que siguieron a la Segunda Guerra Mundial y especialmente los que se gestaron en la última década, han propiciado cambios significativos en las formas en que las personas intercambian información.

En este sentido, la informática ha sido una de las áreas del conocimiento humano que mayor desarrollo ha experimentado.

Este conjunto de técnicas, herramientas y conocimientos, que se engloban en la disciplina informática, permiten el tratamiento automatizado de la información, utilizando computadoras, teléfonos y una gran variedad de dispositivos.

No obstante, este avance vertiginoso, el mismo que propició la denominada "Sociedad de la Información y el Conocimiento", supone retos importantes para proteger y asegurar la información y los datos tanto empresariales como personales, tarea que abarca mucho más que solo la tecnología y que debe sustentarse en un adecuado "Gobierno de la Seguridad de la Información Institucional".

En línea con lo anterior, se debe "asegurar que los recursos del sistema de información -material informático o programas - de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización." Wikipedia http://es.wikipedia.org/wiki/Seguridad_informática

Triada de la seguridad de la información	
Integridad	La información adecuada
Confidencialidad	A las personas adecuadas
Disponibilidad	En el momento adecuado

Bajo esta perspectiva, el modelo de seguridad de la información se puede definir mediante tres conceptos que constituyen los pilares de la llamada tríada de la seguridad, compuesta por la confidencialidad, la integridad y la disponibilidad de la información.

Integridad

El concepto de Integridad de la información, se relaciona con la protección de la exactitud que debe dársele a la información, tanto en su procesamiento como en su almacenamiento. En otras palabras, esta característica busca mantener los datos libres de modificaciones no autorizadas. La violación de la integridad se presenta cuando un individuo, programa o proceso -por accidente o con mala intención- modifica, corrompe o borra parte de los datos.

Como respuesta a estas transgresiones a la integridad, los mecanismos de firma digital, se han convertido en uno de los métodos más fiables para garantizar, al menos en el caso de los documentos electrónicos, que los mismos no hayan sido modificados. Con la aprobación de la Ley de firma digital en nuestro país, se está impulsando en el Poder Judicial la incorporación de tan importante refrendo a los documentos y se espera que en el corto plazo esté siendo utilizada la firma digital en diferentes procesos, como por ejemplo: firma de sentencias, firma de documentos que se envían a otras instituciones, firma de notificaciones electrónicas que se envían

a los Proveedores, certificados de delincuencia, el cual puede ser solicitado a través de Internet y dictamen médico legal que emite la Sección de Patología del Complejo de Ciencias Forenses.

Confidencialidad

La confidencialidad, se refiere a la protección de la información de su divulgación indebida. En este sentido, el Poder Judicial toma en cuenta varios aspectos para determinar la sensibilidad y confidencialidad de la información, como son: el origen racial o étnico de las personas, las convicciones religiosas, espirituales, de vulnerabilidad o filosóficas, datos de carácter personal relativos a la salud o vida sexual, antecedentes delictivos, entre otros.

Disponibilidad

Consiste en permitir el acceso a la información cuando esta es requerida por las personas, procesos o aplicaciones. En este sentido, en el Poder Judicial se han tratado de incorporar en los sistemas de información las principales reglas de accesibilidad, de manera que se facilite el acceso a la información tanto a los usuarios internos de la institución como a cualquier ciudadano, independientemente de sus limitaciones. En el sitio web del Poder Judicial se publica una amplia gama de información, tal como: las sentencias judiciales, el estado y trámite de los expedientes, Actas de Corte Plena y del Consejo Superior, información presupuestaria y de carácter administrativo, lo cual además de facilitar el acceso a la información, promueve la transparencia y facilita la rendición de cuentas de la institución. Actualmente, se está trabajando en el rediseño del sitio web del Poder Judicial, con el fin de mejorar la interfase con los usuarios externos e incorporar nuevos y mejores servicios acorde con las necesidades de los mismos.

En el tema de la disponibilidad, es trascendental la definición de planes de contingencia que incluya la disponibilidad de sistemas redundantes y fuentes alternas de energía que minimicen las fallas y permitan garantizar al usuario la continuidad del servicio. Para tal efecto, en el Poder Judicial se han identificado los sistemas más críticos y para los mismos se han establecido esquemas de replicación.

De igual forma, en todos los sistemas se tienen definidos esquemas de respaldos de información, de manera que ante cualquier desperfecto o violación a la integridad de los datos se pueda recuperar la información.

El sistema ha ido evolucionando acorde con los cambios y exigencias de la organización y los usuarios, lo que conlleva retos importantes en materia tecnológica para atender la demanda de nuevos requerimientos y nuevos mecanismos para administrar, acceder y proteger la información. Por ejemplo, la "Oralidad" en los procesos judiciales, que implica el uso de audio y video, involucra el surgimiento de interrogantes sobre la forma de ocultar la información, ya que en vez de realizar la encriptación de un dato en modo de carácter, podría ser necesario ocultar una imagen o distorsionar un sonido. Además, se incrementan los requerimientos de infraestructura tecnológica con la incorporación de nuevos dispositivos y se requiere mayor capacidad para manejar, transmitir y almacenar grandes volúmenes de información, así como determinar otras alternativas para realizar las búsquedas de información de manera eficiente.

Ambiente de seguridad de la información

Al realizar sus operaciones diarias, las instituciones como el Poder Judicial, deben enfrentarse a un sinnúmero de leyes, reglamentos, tecnologías y requerimientos, mismos que constantemente están cambiando a un ritmo vertiginoso.

Todas estas fuerzas, deben formar parte del ambiente de seguridad de la información que debe definirse a lo interno de las organizaciones.

Como parte de este ambiente, hay que tener en cuenta que en la mayoría de las instituciones públicas, los activos más valiosos no siempre son tangibles, refiriéndose más a temas como la imagen, la confianza de los participantes en la Administración de Justicia, entre otros elementos.

Así las cosas, la definición clara de estándares, procedimientos y guías en materia de seguridad de la información, deben tomar en cuenta a todas estas fuerzas y debe contener especialmente, los roles y responsabilidades de aquellos que utilizan la información

institucional, así como planes de corto, mediano y largo plazo para asegurar este valioso activo.

Este marco de definición de la seguridad institucional, evidentemente debe incluir un elemento técnico, donde hay varios aspectos que deben tomarse en cuenta, tales como:

- Definir una arquitectura de información que incorpore esquemas de seguridad acorde con el tipo de información y transacciones que se realizan. Dicho esquema debe ser sometido a pruebas de calidad robustas que aseguren su eficiencia.
- Incorporar algoritmos de encriptación de datos, que aseguren la confiabilidad y protección de la información sensible, previniendo que personas no autorizadas sean capaces de ver o modificar dicha información.
- Incorporar la firma digital en el intercambio de documentos electrónicos, en los cuales se requiera asegurar que el contenido no ha sido alterado.
- Proteger los equipos servidores de datos, las bases de datos, y las redes de las instituciones, de accesos indebidos, mediante la incorporación de dispositivos de seguridad de *hardware* y *software,* pues constituyen un atractivo para los delincuentes cibernéticos.
- Definir esquemas de respaldos de la información y esquemas de contingencia, para asegurar la continuidad del servicio y la disponibilidad de la información.

Por consiguiente, es necesario que las aplicaciones, los datos y la infraestructura tecnológica, se encuentren protegidos bajo un esquema de seguridad definido en el marco de políticas y procedimientos formalmente establecidos.

Protección de datos

La protección de datos es un conjunto de instrumentos de índole jurídico que permite proteger la intimidad y otros derechos de imagen de cada individuo: tema que cobra especial relevancia en esta era de información digital.

En nuestro país se han realizado esfuerzos orientados a garantizar la protección de datos, algunos de los cuales han fructificado, y otros han quedado o se encuentran en la corriente legislativa. Como ejemplos concretos se pueden citar:

El Habeas Data

La Sala Constitucional ha desarrollado el derecho de imagen como una extensión del derecho a la intimidad, protegido constitucionalmente en el artículo 24 de la Constitución Política, cuyo fin es resguardar el ámbito o esfera privada de las personas del público, salvo autorización expresa del interesado.

De esta manera, se limita la intervención de otras personas o de los poderes públicos en la vida privada de las personas; esta limitación puede encontrarse tanto en la observación y en la captación de la imagen como en la difusión posterior de lo captado sin el consentimiento de la persona afectada.

Con base en estos criterios jurídicos, el Poder Judicial ha recibido varios recursos de Amparo, en los cuales se plantea la violación a la intimidad de las personas, lo que ha llevado a la institución a ser más rigurosa en los controles y procedimientos establecidos para no violentar este derecho, así como incorporar herramientas tecnológicas que apoyen el proceso.

Proyecto de Ley de Protección de la persona frente al tratamiento de sus datos personales

Mediante el mismo, se pretende proteger los derechos a la intimidad y a la autodeterminación informativa, para garantizar una efectiva protección del ciudadano frente a los cambiantes sistemas computadorizados de almacenamiento y distribución de datos. Si bien se han presentado en la Asamblea Legislativa varios proyectos de ley al respecto, aún no se cuenta con una ley que permita prevenir el uso indebido de la información de las personas.

Reglas de Heredia

Estas fueron definidas en un Congreso que se llevó a cabo en nuestro país en Heredia el 9 de julio del 2003 y giran en torno a la protección

de datos en el ejercicio de la justicia. Como ejemplo se citarán algunas de las reglas:

Finalidad

Regla 1. La finalidad de la difusión en Internet de las sentencias y resoluciones judiciales será: [1]

(a) El conocimiento de la información jurisprudencial y la garantía de igualdad ante la ley;

(b) Para procurar alcanzar la transparencia de la administración de justicia.

Regla 2. La finalidad de la difusión en Internet de la información procesal será garantizar el inmediato acceso de las partes o quienes tengan un interés legitimo en la causa, a sus movimientos, citaciones o notificaciones.

Derecho de oposición del interesado

Regla 3. Se reconocerá al interesado el derecho a oponerse, previa petición y sin gastos, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de difusión, salvo cuando la legislación nacional disponga otra cosa. En caso de determinarse, de oficio o a petición de parte, que datos de personas físicas o jurídicas son ilegítimamente siendo difundidos, deberá ser efectuada la exclusión o rectificación correspondiente.

Adecuación al fin

Regla 4. En cada caso los motores de búsqueda se ajustarán al alcance y finalidades con que se difunde la información judicial. [2]

Balance entre transparencia y privacidad

Regla 5. Prevalecen los derechos de privacidad e intimidad, cuando se traten datos personales que se refieran a niños, niñas, adolescentes (menores) o incapaces; o asuntos familiares; o que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos; así como el tratamiento de los datos relativos a la salud o a la sexualidad; [3] o

victimas de violencia sexual o domestica; o cuando se trate de datos sensibles o de publicación restringida según cada legislación nacional aplicable [4] o hayan sido así considerados en la jurisprudencia emanada de los órganos encargados de la tutela jurisdiccional de los derechos fundamentales. [5]

En este caso se considera conveniente que los datos personales de las partes, coadyuvantes, adherentes, terceros y testigos intervinientes, sean suprimidos, anonimizados o inicializados, [6] salvo que el interesado expresamente lo solicite y ello sea pertinente de acuerdo a la legislación.

Regla 6. Prevalece la transparencia y el derecho de acceso a la información pública cuando la persona concernida ha alcanzado voluntariamente el carácter de publica y el proceso esté relacionado con las razones de su notoriedad. [7] Sin embargo, se considerarán excluidas las cuestiones de familia o aquellas en los que exista una protección legal específica.

En estos casos podrán mantenerse los nombres de las partes en la difusión de la información judicial, pero se evitarán los domicilios u otros datos identificatorios.

Regla 7. En todos los demás casos se buscará un equilibro que garantice ambos derechos. Este equilibrio podrá instrumentarse:

(a) En las bases de datos de sentencias, utilizando motores de búsqueda capaces de ignorar nombres y datos personales;

(b) En las bases de datos de información procesal, utilizando como criterio de búsqueda e identificación el número único del caso.

Se evitará presentar esta información en forma de listas ordenadas por otro criterio que no sea el número de identificación del proceso o la resolución, o bien por un descriptor temático.

Regla 8. El tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad, sólo podrá efectuarse bajo el control de la autoridad pública. Sólo podrá llevarse un registro completo de condenas penales bajo el control de los poderes públicos. [8]

Regla 9. Los jueces cuando redacten sus sentencias u otras resoluciones y actuaciones, [9] harán sus mejores esfuerzos para evitar mencionar hechos inconducentes o relativos a terceros, buscaran sólo mencionar aquellos hechos y datos personales estrictamente necesarios para los fundamentos de su decisión, tratando no invadir la esfera íntima de las personas mencionadas. Se exceptúa de la anterior regla la posibilidad de consignar algunos datos necesarios para fines meramente estadísticos, siempre que sean respetadas las reglas sobre privacidad contenidas en esta declaración. Igualmente se recomienda evitar los detalles que puedan perjudicar a personas jurídicas (morales) o dar excesivos detalles sobre los moda operandi que puedan incentivar algunos delitos. [10] Esta regla se aplica en lo pertinente a los edictos judiciales.

Regla 10. En la celebración de convenios con editoriales jurídicas deberán ser observadas las reglas precedentes.

Definiciones

Datos personales: Los datos concernientes a una persona física o moral, identificada o identificable, capaz de revelar información acerca de su personalidad, de sus relaciones afectivas, su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio físico y electrónico, número nacional de identificación de personas, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad o su autodeterminación informativa. Esta definición se interpretara en el contexto de la legislación local en la materia.

Motor de búsqueda: son las funciones de búsqueda incluidas en los sitios en Internet de los Poderes Judiciales que facilitan la ubicación y recuperación de todos los documento en la base de datos, que satisfacen las características lógicas definidas por el usuario, que pueden consistir en la inclusión o exclusión de determinadas palabras o familia de palabras; fechas; y tamaño de archivos, y todas sus posibles combinaciones con conectores booleanos.

Personas voluntariamente públicas: el concepto se refiere a funcionarios públicos (cargos electivos o jerárquicos) o particulares que se hayan involucrado voluntariamente en asuntos de interés público (en este caso se estima necesaria una manifestación clara de renuncia a una área determinada de su intimidad)

Anonimizar: Esto todo tratamiento de datos personales que implique que la información que se obtenga no pueda asociarse a persona determinada o determinable.

Alcances

Alcance 1. Estas reglas son recomendaciones que se limitan a la difusión en Internet o en cualquier otro formato electrónico de sentencias e información procesal. Por tanto no se refieren al acceso a documentos en las oficinas judiciales ni a las ediciones en papel.

Alcance 2. Son reglas mínimas en el sentido de la protección de los derechos de intimidad y privacidad; por tanto, las autoridades judiciales, o los particulares, las organizaciones o las empresas que difundan información judicial en Internet podrán utilizar procedimientos más rigurosos de protección.

Alcance 3. Si bien estas reglas están dirigidas a los sitios en Internet de los Poderes Judiciales también se hacen extensivas -en razón de la fuente de información- a los proveedores comerciales de jurisprudencia o información judicial.

Alcance 4. Estas reglas no incluyen ningún procedimiento formal de adhesión personal ni institucional y su valor se limita a la autoridad de sus fundamentos y logros.

Alcance 5. Estas reglas pretenden ser hoy la mejor alternativa o punto de partida para lograr un equilibrio entre transparencia, acceso a la información pública y derechos de privacidad e intimidad. Su vigencia y autoridad en el futuro puede estar condicionada a nuevos desarrollos tecnológicos o a nuevos marcos regulatorios.

Ley No. Nº 8454, Ley de Certificados, Firmas digitales y documentos electrónicos

Aplica a toda clase de transacciones y actos jurídicos, públicos o privados, salvo disposición legal en contrario, o que la naturaleza o los requisitos particulares del acto o negocio concretos resulten incompatibles.

En la misma, se faculta al Estado y a todas las entidades públicas para que puedan utilizar los certificados, las firmas digitales y los documentos electrónicos, dentro de sus respectivos ámbitos de competencia.

Comisión para la Implementación de las Reglas de Heredia:

En el año 2004 fue constituida esta comisión por Corte Plena en sesión Nº 036, Artículo XIII, con el fin de garantizar la transparencia y el respeto de los datos personales de quienes interactúan con la Administración de la Justicia, la cual estaba integrada por varios magistrados y fue presidida por el Magistrado Adrián Vargas, dicha comisión realizó un estudio sobre la información que se maneja a lo interno del Poder Judicial y definió un Reglamento sobre la protección de datos, utilizando como base las Reglas de Heredia que fueron establecidas para utilizarlas como referencia a nivel Internacional.

Implementaciones técnicas para brindar protección de datos

Con base en los criterios antes expuestos, de previo a la divulgación de sentencias se lleva a cabo la revisión de información de las víctimas que puede ser considerada de carácter privado, por lo que es necesario protegerla de accesos no permitidos.

Al respecto, se han realizado esfuerzos institucionales para ocultar los datos en materia judicial, mediante el uso mecanismos, tales como:

Identificación de expedientes confidenciales: se refiere a expedientes que se les da un trato confidencial y por consiguiente su información solo es accesible por las partes involucradas en el proceso judicial correspondiente.

Editor de textos propiedad del Poder Judicial: esta herramienta permite ocultar información de las sentencias, cuando esta ha sido calificada como de tipo confidencial. De esta forma se podrá divulgar información sin que los datos sensibles puedan ser visualizados por personas ajenas al proceso judicial.

Esquemas de seguridad en los sistemas de información: permiten establecer un acceso restringido a la información, admitiendo su consulta únicamente a las personas involucradas en el proceso judicial y su rigurosidad depende del nivel de confidencialidad de los datos.

Inicialización de nombres: significa que para la publicación de sentencias el personal del Centro Electrónico de Información Jurisprudencial y del Centro de Jurisprudencia Judicial, modifican "manualmente" los nombres de las partes incluyendo únicamente las iniciales de sus nombres –así Jorge Pérez Molina aparecería como JPM-. Complementariamente a este procedimiento se eliminan números de cédula y otros datos que permiten identificar a una persona. Esto se aplica en casos de: Violencia Doméstica, Abusos Sexuales, en casos donde se mencionan los datos de menores, adultos mayores enfermos de sida o en sentencias asociadas con expedientes confidenciales.

También se inicializan los nombres y se excluyen los datos de coadyuvantes, adherentes, terceros y testigos intervinientes, incluidos los parientes de la víctima. En el procedimiento de inicialización se presentan algunas excepciones, como por ejemplo, individuos que solicitan no ocultar sus datos y nombres de directores, jefes o personas que ocupan cargos públicos, en cuyo caso la información no debe ser ocultada, por cuanto se considera de interés público.

Es importante señalar que los despachos Judiciales generan diariamente gran cantidad de información que debe cumplir con los tres conceptos de seguridad antes definidos: Integridad, Confidencialidad y Disponibilidad, sin embargo en algunos casos los procedimientos utilizados para ocultar la información no son 100% efectivos.

En el caso particular de la jurisprudencia que es divulgada a través del Sitio Web del Poder Judicial, se presentan situaciones en las que

los mecanismos utilizados para ocultar la información pueden limitar la comprensión de la resolución, particularmente en los casos donde participan varios imputados y podría presentarse una coincidencia en las iniciales de sus nombres o la encriptación de los datos no permite una lectura comprensible, con lo cual se ve afectado el principio de exactitud.

Si bien se han realizado esfuerzos para implementar un proceso automático de encriptación de la información, no se ha logrado encontrar una herramienta que permita realizar esta función de forma ágil, ya que la misma debe ser capaz de proteger los nombres y datos que identifiquen a las partes, pero omitiendo los nombres de jueces, autores citados, entre otros. Además deberá ser capaz de detectar cualquier dato que rebele la identidad de un individuo, como identificación de puesto desempeñado, títulos nobiliarios, apodos, características físicas, entre otros e identificarlos aún cuando se presenten con algún error de escritura. Por consiguiente, en el proceso de ocultar información predomina una actividad "manual", particularmente en el tratamiento de la jurisprudencia que se pone a disposición de los usuarios externos, lo cual de alguna forma afecta disponibilidad de la información.

Conclusión

Como se puede apreciar son bastantes los esfuerzos que se han realizado a nivel nacional en materia de seguridad de la información y protección de datos. Las normas aprobadas en nuestro país a nivel de la Asamblea Legislativa constituyen pilares para el análisis jurídico y el desarrollo tecnológico de las instituciones y en particular del Poder Judicial, que como institución que administra justicia debe velar por el acatamiento de las mismas. El acceso a la información se convierte en un tema neurálgico para el desarrollo de la sociedad, y por lo tanto merece el tratamiento adecuado con el fin de salvaguardar la seguridad y protección de la información. Los esfuerzos que en este sentido se han realizado no son aún suficientes y se requiere de los aportes de las áreas del conocimiento pertinente, en este caso "el derecho" y "la tecnología" para encontrar soluciones oportunas y eficaces antes las necesidades emergentes.

Protección de datos en el Registro Nacional

Johnny Chavarría Cerdas

La idea es presentarles lo que el Registro Nacional ha venido haciendo en materia de aseguramiento de la información como un caso vivo. Hablar del marco estratégico partiendo del hecho de que este debe venir desde los niveles más altos de la organización; el tema de la seguridad en el caso del Registro Nacional es un tema medular. También vamos a conversar sobre los antecedentes, el plan estratégico de aseguramiento de la información y lo que hemos hecho en las distintas áreas de acción, además de lo que logrado en materia de seguridad de la información desde hace cuatro años, el impacto que hemos tenido a nivel de servicio y lo que queda por hacer.

Misión: En el Registro Nacional de Costa Rica protegemos los derechos inscritos, ofreciendo seguridad jurídica prestando servicios de calidad, con recurso humano calificado y tecnología idónea.

Hablando desde el punto de vista estratégico, desde el marco de una organización que le da cabida al valor de la seguridad de la información. En el Registro Nacional protegemos los derechos inscritos, ofreciendo seguridad jurídica prestando servicios de calidad, con recurso humano calificado y tecnología idónea.

Entonces desde nuestra misión misma se plantea lo que es la importancia de la seguridad de información para el Registro Nacional y desde ahí empezamos a esbozar una serie de planes, de acciones, de planteamientos estratégicos, tácticos y operativos para poder implementar esa misión. Es un plan estratégico integrado por el Ministro de Seguridad, la Junta Administrativa y la dirección de todas las partes de la empresa. El Registro Nacional generó el primer plan estratégico en tecnologías de la información y telecomunicación en el que se definieron tres grandes pilares para la sostenibilidad del sistema.

Durante 4 años se ha estado haciendo revisiones informáticas, se definieron tres vértices:

- Garantizar la continuidad de los servicios a los costarricenses, que no tenga obsolescencia tecnológica, sin vulnerabilidades o suspensiones sino que se tuviera el tema de continuidad del negocio.
- El segundo pilar que desde el 2005 venimos trabajando en el tema de gobierno corporativo, que ahora se le llama gobierno de las tecnologías, de cómo administramos la cuestión de las ISO, de la administración de proyectos.
- El tercer pilar del plan estratégico era crear un sistema de único registro que se llama SUR, estamos apostando en el desarrollo del nuevos sistema único de registro donde vamos a ofrecer una plataforma única de servicios al ciudadano que estamos trabajando en un convenio con el Banco de Costa Rica.

El tema de gobierno es un pilar fundamental respecto a la seguridad informática y por lo fundamental que es, se hizo un plan estratégico de aseguramiento de la información y se desagrego entre otros planes, primero para darle un reconocimiento al esfuerzo que estaba haciendo la Dirección de Informática y el Registro como un todo en materia de seguridad de la información.

Segundo buscar patrocinadores adherirlos al plan estratégico de aseguramiento de la información para comprometer recursos, para comprometer políticas porque necesitábamos padrinos para llevar a cabo proyectos de tecnologías de la información, porque muchos de los

planes que están contemplados aquí en el tema de gobierno de la tecnología se ejecutan a través del PAO o POI es una cuestión de presupuesto.

El plan estratégico de aseguramiento de la información tiene 4 columnas: seguridad externa (antispam, antivirus, filtros, etc.) seguridad interna, de seguridad física, de seguridad lógica y de organización.

El tema de descubriendo y redescubriendo las vulnerabilidades, es un tema en el que hay que hacer mucho énfasis, porque la seguridad de la información es un proceso, un proceso vivo, un proceso grande, un proceso que tiene que estar en constante evolución, por lo que estamos en un proceso permanente de auditorías para ver como estamos. Otro tema es el de la cultura organizacional, se puede tener el mejor sistema, la mejor tecnología, los mejores equipos, si no se hace un proceso de concientización de cambio cultural, no se puede tener seguridad de la información.

Antecedentes

En el año 2005 se generó un plan estratégico de desarrollo de las tecnologías de la información y telecomunicación, actualizado en el 2008 y avalado por la Junta Administrativas. A finales del 2006 se trabajó en un diagnóstico del cuál surgió el plan estratégico de aseguramiento de la información, comentado anteriormente.

El el plan estratégico de aseguramiento de la información es un proceso dinámico que está en constante cambio, así que en el 2006 se generó una primera versión del plan, en el 2009 es actualizado con miras hacia el 2013 tomando en cuenta las nuevas amenazas. Algunas áreas de acción definidas para la seguridad lógica es proteger todo lo que es el perímetro del Registro con *Firewall*, lo que son las oficinas regionales se logró un nivel bastante seguro, se hizo una fuerte inversión para mejorar los sistemas de comunicación. El filtrado por Internet hasta ahora no hemos sufrido ningún ataque, se desarrolló un programa de autenticación que es un proyecto que se basa en tecnología triangulada.

Tenemos el tema de las tarjetas porque antes se daba mucho el fraude registral cuando alguien registraba una propiedad se levantaba

el fulano, alguien hacia una operación y el fulano decía no era yo, ahora en el momento que alguien va a trabajar en su computador tiene que introducir una tarjeta en el lector electrónico, entonces ya nadie puede evadir su responsabilidad. Eso nos ha permitido controlar un poco las denuncias por fraudes registrales.

En el sitio web algo tan sencillo como incorporar el uso del *Captcha* porque nosotros sufríamos muchos ataques de *Hobs*, el sitio web estaba colapsado, el sitio era uno de los peores del sistema y ahora estamos en el cuarto lugar de la encuesta del INCAE de 110 instituciones, el punto es que pasamos del oscurantismo total a tener un poco de visibilidad implementando algunas cosas y hacer las cosas visibles después de ver lo que había pasado y revisar lo que podíamos hacer.

En la parte de seguridad física se desarrolló un proceso de credencialización, las tarjetas para entrar a las diferentes áreas del Registro Nacional, hay áreas que además de la tarjeta se necesita la huella digital, a la sala de cómputo se necesita también la huella digital. La credencialización ha servido para implementar lo que es el control de asistencia, entonces lo utilizamos con doble propósito.

Hay 60 cámaras monitoreando el Registro Nacional, hay una sala de monitoreo con grandes pantallas y gente especializada que ven todo lo que está pasando, además con la sala de monitoreo se controlan las puertas y se activan las puertas y se encienden las alarmas para que la gente siga los protocolos de evacuación.

El tema de riesgos se ha estado trabajando, se han hecho auditorías de seguridad en el año 2007, 2008, 2009 para asegurar el trabajo y la información. La ingeniería social ha sido un tema que se ha trabajado mucho, se ha dado capacitación a los empleados, a los abogados se les han dado charlas y se ha publicado en una revista que se llama derecho registral del Colegio de Abogados, tenemos una revista interna y una digital que circula en el Registro y a través de de las cuales se está haciendo conciencia de esa cultura que se requiere.

En el tema de continuidad de negocios tenemos un plan que no estamos muy contentos porque le falta mucho al plan, pero hemos venido trabajando desde el plan estratégico del 2005 venimos sembrando,

sembrando y sembrando, cuando compramos equipos lo compramos redundante y con posibilidad de crecer para que un momento podamos pasar la línea y llevar esos equipos a un data center por ejemplo para manejar el tema de disponibilidad y en el tema de gestión de incidentes también tenemos que trabajar.

Todas esas áreas de acción por decirlo de laguna forma tiene que estar cubiertas por capas, una de esas capas es el tema de procedimientos y las políticas. A nivel de Registro las políticas de aseguramiento de la información que es un grupo de 25 políticas fueron aprobadas directamente por la junta administrativa, por la Ministra de Justicia. Hemos seguido las políticas y trabajado en el tema de procedimientos para obtener la certificación de ISO 9000 para el departamento de informática y la finalidad no es la certificación es la confianza que eso puede transmitir al ciudadano.

Entre los factores externos tenemos las normas de la Contraloría General de la República que nos habla mucho del tema de seguridad nos potencia por un lado y nos compromete por otro. El proyecto de ISO 9001estamos trabajando para certificar la dirección de informática todos los procesos en ISO 900.

El SEVRI: con la nueva ley de control interno, estamos trabajando muy fuerte en la capacitación del ISO 27001 porque quisiéramos que algunos de los procesos más críticos, no en tecnología sino en uso del negocio, tenemos que generar confianza en el ciudadano; para nadie es un secreto la fama que ha venido arrastrando el registro, para nosotros es importante cambiar esa mentalidad del público para gestionar como una marca de confianza. Tenemos funcionarios más conscientes, la gente denuncia más por lo que se han reducido los casos de actuación dudosa. Contamos con mayor seguridad física. Hemos fortalecido toda nuestra estructura tecnológica con equipos de alta tecnología, todo lo que les mencionaba del tema de tarjetas, de monitoreo.

Lo que hemos hecho en un período tan corto porque venimos gestionando desde el 2005 ya está dando lo frutos, estamos muy claros de lo que tenemos que hacer, ya marcamos el rumbo y a hacia eso vamos.

Protección de datos en el Tribunal Supremo de Elecciones

Dennis Cascante Hernández

La organización para el proceso de elecciones del 2006, y los esfuerzos por la seguridad de la información, por la seguridad informática son el tema de esta conferencia, que si comparamos con el proceso de las elecciones del 2002 hay una gran evolución, un cambio radical. De lo que vamos a hablar ahora es un poco de cómo se transmitieron los datos en la noche de las elecciones propiamente en el 2006.

No quisiera dejar por fuera el tema de control, porque un control si no está fundamentado en el tema del negocio en el eje estratégico del negocio adecuadamente alienado con los objetivos del negocio simplemente se vuele letra muerta. Podríamos encontrarnos en una situación en la que implementamos un determinado control pero no conocemos la efectividad que tiene para controlar lo que queremos de nuestro negocio.

- ISO 17799: 2005 (27002). Como referencia uno de los principios que tomamos fue la norma de ISO "Información es un activo que como el resto de los activos comerciales importantes, tiene valor para la organización y por lo tanto debe ser apropiadamente protegido".

Y eso de ser protegida apropiadamente nos lleva a pensar que tipo de información es, a que proceso pertenece, que tan sensible es esa información y así definimos que tipo de riesgos tiene y qué tipo de protección le debemos dar. Es todo un universo de servicios, vamos a adelantar que en ese proceso de captura y procesamiento de esa información, que llegue en tiempo real directamente al Tribunal Supremo de Elecciones, que se publica en el sitio y la que se da a los medios para que sea consumida.

Previamente se documentaron una buena cantidad de interacciones para clasificar dentro de todo lo que es el proceso electoral en subprocesos y agregar un valor e identificar la tecnología que soporta ese proceso para una clasificación, darle su valor estratégico dentro de la organización y al final hacer un análisis de brecha e implementar los controles para cerrar esa brecha.

Características del proceso

- Antecedentes del 2002
- Cambio de Tecnologías
- Transmisión de resultados por Internet
- Alianzas estratégicas en función de lo dispuesto en el código electoral.
- Velocidad y Certeza en resultados preliminares

En todos los procesos anteriores del 2006 se hacían en tecnologías diferentes y para el 2006 se hace un cambio de la tecnología con retos a nivel tecnológico muy importantes.

Otra característica de este proceso del 2006 era el aprovechamiento de Internet, hasta el 2002 se usaba una red particular del gobierno que fue creada con fines educativos particularmente, para el 2006 esta red ya no existía lo que nos quedaba era una red pública.

Dentro de las características de este proceso como ustedes saben el ejercicio del sufragio, del voto se realiza a todo lo largo y ancho del país y el reto era como traer esos resultados en el tiempo adecuado unas dos horas después de cerradas las juntas receptoras, de tal manera que nosotros pudiéramos tener en el sitio principal del Tribunal Supremo de elecciones esos resultados listos para que en la noche de las elecciones pudiéramos tener en tiempo real y filtrarlos a los diferentes medios de comunicación colectivos para que ellos hicieran la difusión.

Un poco lo que se discutía en esa ocasión era que al transmitir por Internet resultados por el medio público fue si el sector financiero puede pasar dinero de manera segura, nosotros podemos pasar la información de manera igual. Entonces ahí empezamos a correr lo que es el análisis para lograr la protección de datos y un aspecto importantísimo que no puedo dejar de mencionar es que a partir de ciertas consideraciones del código electoral, las instituciones públicas prestan cierta colaboración al tribunal para realizar sus procesos. Especial colaboración tuvimos con los proveedores de servicios de Internet hablamos del ICE y RACSA un poco cuál era la dinámica el ejercicio del voto se realiza en todos los centros educativos a lo largo y ancho del país.

Características de los centros de votaciones, los centros educativos, en su mayoría gracias a la fundación Omar Dengo las escuelas contaban con un laboratorio de cómputo con acceso a Internet, de modo que se volvía ese el medio de acceso o mejor dicho el medio de comunicación por excelencia. Por otra parte las oficinas del Tribunal Supremo de Elecciones conectadas eran 13 de esta forma se generó un escenario, la transmisión era por medio de las redes públicas donde el reto era asegurar esa información no solo desde su generación sino también en el transporte, almacenamiento en el Tribunal y en su ubicación.

Técnicamente lo que sucedía la noche de las elecciones después de que las juntas hacían el conteo establecían una conexión a un sitio alterno donde en coordinación con el ICE y RACSA se establecían ciertas características. Partimos de la premisa básica de disponibilidad, integridad y confidencialidad.

Cuando hablamos de disponibilidad es del sitio donde no había ninguna ventana de tiempo que nos permitiera estar ahí porque el pico de transacciones básicamente iba a ser de 2 a 4 horas con la participación de la gente del ICE y de RACSA, se establecieron mecanismos a nivel de infraestructura algo interesante porque teníamos equipo de telecomunicaciones profesional del ICE con sus respectivos proveedores de servicio y en la misma mesa la gente de RACSA con sus respectivos proveedores entonces teníamos dos colaboradores en la misma mesa, dos competidores de un mercado muy particular con cierto músculo en la materia de telecomunicaciones como lo eran ITS y GBM en ese momento tanto así que tuvimos que traer una suerte de arbitraje incluso con los equipos que se utilizaban en ese momento de tal forma que se adecuaran los equipos, había dos proveedores diferentes como el ICE y RACSA respondiendo a las mismas dimensiones de tipo lógico.

A la fecha era la primera vez que lo hacíamos en el país, esto significa que un proveedor de servicios transporta a través de su infraestructura los clientes de servicio de otro proveedor y viceversa, de tal forma que desde la infraestructura física de cualquiera de los dos pudiera accesarse al sitio del Tribunal.

En el camino el tipo de controles habituales área perimetral, a nivel de *framework,* de IPS, filtro de direcciones que podían hacerse dentro de la nube en conjunto con el ICE y RACSA, algunas características particulares del proceso es que evidentemente encriptábamos el medio, a través de certificados digitales que eran controlados por el Tribunal Supremo de Elecciones.

A manera de característica de protección de datos a nivel de confidencialidad planteamos un *quick show* en el medio pero el gran reto era hacer inspección, porque al encriptar la información estos dispositivos se vuelven ciegos para este tipo de información. Cuando yo tengo un IPS y lo que pasa, pasa encriptado pues no van a ver nada. Tuvimos ahí una colaboración de los fabricantes de los dispositivos que usamos para permitir a través de una red local los IPS que utilizamos un túnel y dejar pasar el tráfico interesante.

Después de pasar ese primer nivel de protección venía una disposición interesante especialmente porque estábamos usando tecnología de diferentes fabricantes, por diferentes infraestructuras, diseñadas para que a través de diferentes operativos se pudiera contar con una alta disponibilidad a nivel de Host, de servidores y de bases de datos, etc. Una vez pasada esa primera zona llagaba a una zona de verificación de tecnología de PKI PRO. En otras palabras una vez que el mensaje atravesó esa primera línea de defensa antes de ser procesada por diferentes aplicaciones del Tribunal se verificaba la identidad de la máquina que estaba al otro lado y del usuario que estaba haciendo la transmisión.

Básicamente aquí quisiera resaltar un punto importante en el tema de protección de datos, cuando hablamos de protección de datos es necesario que la seguridad se establezca en todos los niveles tanto procedimental, de infraestructura, como de los equipos, uno de los retos que teníamos era que los software apuntarán a escribir código que no solamente tuviera la funcionalidad que se esperaba sino que fuera parte de la validez de los usuarios, se hacía a nivel de infraestructura y de los aplicativos leyendo los certificados digitales.

Estos certificados digitales eran construidos por la infraestructura del Tribunal, la cual estuvo lista para octubre del 2005, más o menos dos semanas antes de que se aprobara en segundo debate la ley de firma digital y una vez hecho todos esos procesos de verificación el dato podía pasar a los niveles superiores. Sobre la disponibilidad de la información una infraestructura básicamente robusta, lo que hacíamos era aprovechar las bondades de la infraestructura del ICE y de RACSA para pasar los datos tanto al sitio principal como al sitio alterno de procesamiento.

La importancia de la dimensión estratégica de la concordancia entre los mecanismos de protección y el objetivo del negocio, se da básicamente en la implementación de los controles, no se puede tener sin antes hacer una valoración del riesgo asociado a procesos que previamente han sido clasificados dentro del negocio, con la visibilidad o noción estratégica de la continuidad de negocios.

Controles generales

- Integridad de la información
- Firma Digital
- Confidencialidad
- Mecanismos de encripción
- Disponibilidad
- Sistemas distribuidos

Recapitulando un poco en los retos que se presentaban, era pasar la información con la firma digital, ningún dato se podía transmitir sí la persona encargada no lo firmaba digitalmente, ningún corte se enviaba a la prensa si no estaba firmado digitalmente, ningún dato se almacenaba en la base de datos si no estaba firmado digitalmente, estábamos transmitiendo por medios ordinarios de comunicación por lo que se necesitaba saber si la información que se estaba recibiendo estaba suscrito por el Tribunal Supremo de Elecciones. En el tema de confidencialidad estaba de la encripción y en la disponibilidad que había.

Controles específicos

- Infraestructura de Telecomunicaciones
- Proveedores de Servicios
- Infraestructura de Servidores y SO
- Infraestructura de Almacenamiento
- Sitio de Procesamiento Alterno de Datos
- Servicios para la Prensa

Sobre infraestructura de almacenamiento lo más destacable ahí es que toda la información almacenada estaba firmada digitalmente lo que podía garantizar a través del tiempo que esos datos no puedan extraerse de la base de datos y podíamos verificar si alguien lo modifico. El sitio alterno de procesamiento de datos y los servicios a la prensa que en realidad en esa oportunidad las novedades eran la publicación de resultados en tiempo real.

Hacíamos una evaluación permanente: simulacros y pruebas métricas, procedimientos documentados en detalle, ordinarios, contingencia, monitoreo y administración; gestión de riesgos y análisis de vulnerabilidades, *Pen test, ethical hacking,* etc.

Otras características de ese proceso

Un proceso de evaluación permanente, y debe tener la implementación de métricas, la clasificación de los procesos, la clasificación de los riesgos y la clasificación de los controles para mitigar ese riesgo que traen el tema de tecnología.

El tema procedimental que ya les mocionaba antes, la seguridad no es solo a nivel tecnológico, sino que es a nivel de negocio, a nivel estratégico, estaban todos los participantes, todos los tecnólogos que tenían que cumplir un rol en determinado proceso, ya sea ordinario o extraordinario, cualquier tipo de conductas y comportamientos de los procesadores debían estar totalmente probadas y documentadas. El análisis de vulnerabilidades, el registro es indispensable.Aquí lo importante era crear la conciencia de que los controles que implementamos en tecnología lo que hacían era un riesgo aceptable de acuerdo a los criterios de las altas jerarquías del Tribunal.

A grandes rasgos este es el recorrido de los controles aplicados en el tema de protección de datos en los procesos electorales de transmisión y publicación de los resultados provisionales de la elección 2006.

Protección de datos en la Contrloría General

Joaquín Gutiérrez Gutiérrez

La Contraloría empezó hace ya bastantes años en un proceso de inmersión en la seguridad informática, iniciamos con equipos básicos de protección: Un Firewall y un enrutador con funcionalidades de seguridad. Poco a poco fuimos adquiriendo tecnología especializada en seguridad informática. En un momento determinado nos dimos cuenta de un punto esencial, y es que el eslabón más débil de la cadena de la seguridad informática lo constituyen las personas (los funcionarios) y es ahí donde la tecnología no puede llegar. Citemos como ejemplo el uso inadecuado del correo electrónico, el uso inadecuado de la estación de trabajo, en su tiempo el uso inadecuado de los diskettes luego de los CD´S y ahora las memorias USB. Esto no se puede proteger con tecnología, se debe proteger con concientización de los usuarios. De tal forma que tomamos la decisión de asegurar ese eslabón mediante la creación de un manual de lineamientos de seguridad para establecer cómo se debe utilizar la tecnología. Ya para el año 2002 nos avocamos a empezar con este proyecto.

Antecedentes

En el 2003 después de todo un año de trabajo, se emitió la primera versión del "Manual Institucional de Políticas de Seguridad en Tecnologías de la Información" así se llamó. Objetivo: normar la utilización de las tecnologías de información para minimizar situaciones de riesgo sobre la plataforma tecnológica.

Este manual de seguridad tiene fundamento en un documento base elaborado por el PNUD. El equipo de trabajo estuvo formado por personas del área administrativa, específicamente de Recursos Humanos, de la Proveeduría, del área Legal, de la Unidad de Tecnologías de la Información (UTI), del área sustantiva "FOE", Fiscalización Operativa y Evaluativa logramos obtener apoyo de la Auditoría Interna de la Contraloría en carácter de asesoría.

Cuando el documento estuvo listo, se le entregó personalmente a cada funcionario, se impartieron charlas de sensibilización enfocadas en los riesgos inherentes del uso inadecuado de las tecnologías por parte de los funcionarios. Se enviaron correos electrónicos masivos, se publicaron en las pizarras informativas de la institución afiches relativos al tema.

Ahora bien, nos planteamos en ese entonces la necesidad de contar con una garantía de que las políticas se iban a acatar y que iban a ser funcionales, ¿pero cómo?.

Lo primero era tener usuarios consientes en el uso adecuado de la tecnología, esto asociado a un esquema sancionatorio. Lo segundo se podría lograr mediante un esquema de monitoreo de la aplicabilidad de estas políticas. Era necesario saber si lo contemplado en el papel era totalmente aplicable y realizable para la Contraloría.

El documento de políticas; como elemento vivo que es, ha evolucionado con el tiempo y constantemente se hacen valoraciones del mismo para verificar posibles cambios adiciones o eliminación de alguna política. Por ejemplo cuando iniciamos con su aplicación, no existían los ataques de "back doors", la negación de servicio ni el famoso phishing. Todo esto ha tenido que ser incorporado como parte del documento.

Igual empezamos a incursionar en las tecnologías inalámbrica WiFi, y todos los riesgos de seguridad que esta tecnología implica, la red de telefonía y ahora el equipo periférico que utilizan las personas y que lo tienen para conectarse a las redes de datos: teléfonos móviles, Ipods, y portátiles personales. Hemos tenido que definir esquemas de estratificación de redes, considerando redes seguras e inseguras (públicas). Todo esto paralelo al establecimiento de normativa y de reglas para el uso adecuado de las mismas.

En el documento, las políticas se dividen en dos tipos: Las de acatamiento para usuarios y las de acatamiento para la UTI. El documento se revisa constantemente por un equipo de la UTI y con un grupo interdisciplinario que nos aportan los conocimientos o las experiencias que ellos tienen.

Este documento está estructurado en los siguientes capítulos: Políticas generales, políticas en el uso de contraseñas *(passwords),* políticas del uso de Internet, políticas de uso del correo electrónico, políticas de acceso conmutado a la red, éstas son muy importantes porque así se pueden controlar riesgos como *" back doors"*: Habían usuarios que tenía una computadora conectada a la red con todas las políticas y estándares de seguridad y además en forma simultánea se conectaban a internet por medio de modem o ahora por medio de la red 3G (Kolbi) datos. Con esto se burlaban todas las medidas de seguridad debido a esa segunda conexión sin ningún control.

Otro capítulo es el de Políticas con el uso de las cuentas conmutadas para el acceso a internet: ya no se aplica mucho, sin embargo en un inicio funcionaba para los usuarios a los cuales nosotros les asignamos cuentas para que cuando llegaran a la casa pudieran utilizar el Internet. Había que regular el uso de este tipo de conexiones. Se consideran también dentro de este documento, políticas en el uso de tecnologías de información y comunicaciones y políticas en el control de virus informáticos. Es importante hacer notar que las políticas nos facilitan a la unidad de Tecnologías la adquisición de la tecnología específica en seguridad.

Políticas de seguridad institucional, como se van a instalar los *Firewalls*, la implementación de las redes con base en la importancia, la sensibilidad de cada uno de los segmentos de red, todo esto se incluyó en un capítulo específico dentro del documento, políticas de acceso a los servidores. Acá controlamos aspectos como los accesos tipo *Telnet*, los cuales son inseguros porque los passwords no van encriptados y en ese caso es mejor que se utilicen accesos tipo *"ssh"* que tienen password encriptados. Por ejemplo si el administrador de la base de datos se está *"logueando"* y hay alguien husmeando con un sniffer, puede perfectamente ver el password que le da y se puede apoderar de toda la información de la base de datos.

Políticas de servicio para el uso de nombres de dominio, políticas para el desarrollo de sistemas de información (este es todo un capítulo importantísimo). Políticas de utilización en las bases de datos, todos los controles que se deben establecer en este sentido, políticas en los servicios Web, políticas en la administración y control ambiental del centro de computo.

El uso de conexiones inalámbricas internas: como les decíamos, hay funcionarios que requieren conectarse desde su computadora personal y dispositivo móvil a internet, pero para esto hay todo un procedimiento definido. Establecimos dos tipos de redes. Una para dar acceso regulado a Internet, básicamente (consultores y funcionarios con equipos personales) y otra para acceso a la red interna. En este último caso el acceso debe ser con un equipo nuestro, porque sí no estamos metiendo un equipo ajeno a la red interna, con las consecuentes implicaciones y riesgos de seguridad.

Ahora estamos trabajando con el tema del teletrabajo. Los funcionarios se van a trabajar a las casas, y tenemos que garantizar que el acceso sea seguro. En este sentido se les instala una serie de programas adicionales de seguridad, como firewall personal, control de acceso a Internet, y VPN. El lineamiento de la Contraloría es, sí la gente se va a teletrabajar, tiene que tener una laptop Institucional. No permitimos el uso de equipos personales para el trabajo ya que al estar conectándose vía VPN, le estamos dando acceso a la red interna, y si no sabernos con que programas de seguridad cuenta el equipo,

no podemos garantizar el acceso seguro. Además este tema también tiene que ver con el software que la contraloría utilice y sobre el cual también ha pagado licenciamiento.

La ventaja a nivel de seguridad que tiene la red inalámbrica es el certificado digital que está incorporado como parte de esta y es lo más seguro para efectos internos. Un tema que estamos viendo actualmente y que es de tecnología, es que alguien se le puede conectar a la red por medio de un *Access Point* que este abierto, un hacker puede ver un access point y entrar a la red de la Contraloría. Nosotros permanentemente tenemos registros de ataques (o intentos de ataques) desde muchos lugares. Este es un tema actualmente muy riesgoso y por el cual estamos incorporando tecnología que se llama "NAT" o "NAP", que es control de acceso al medio. Es decir poder controlar quién se pega a la red, tanto alámbrica como inalámbrica. Poder garantizar el estado de "salud" del equipo y negar el acceso si no cumple con las políticas de seguridad establecidas por nosotros.

Dentro de estas normas técnicas tenemos el marco de seguridad y en a acatamiento de éstas estamos desarrollando un sistema de administración y control de contingencias. En este sistema se manejan niveles de criticidad de recursos, porque si no sabemos ni conocemos los recursos que tenemos no sabremos qué proteger. No podemos disparar para todo lado, tampoco podemos proteger todo. Es necesario también conocer el riesgo asociado, manuales de escalamiento, entre otros.

Parte de este sistema es el documento de lineamientos de seguridad de TIC, revisado semestralmente, genera la estructura de un comité de seguridad al cual se le asigna responsabilidad relacionda a cada uno de los miembros de este comité de seguridad, además, empieza a funcionar formalmente la figura del oficial de seguridad como elemento importante dentro de este proceso de construcción de políticas y lineamientos de seguridad.

Por otro lado, las auditorías con respecto a la seguridad, son un punto sensible, principalmente si se consideran los costos asociados. Contratar una empresa para que haga una auditoría en todos tus elementos de seguridad implica una erogación importante de dinero y a la fecha la tenemos pendiente de hacer.

El costo de la implementación de las normas técnicas es muy elevado y en la Contraloría como administración activa, sabemos que hay instituciones muy diferentes. Una municipalidad a veces tiene un solo informático, a veces no cuenta con este recurso y tiene que contratar el servicio de TI. Este es un tema que es caro y que por lo general se divide en dos o tres etapas: como ejemplo, en el caso de la seguridad primero se hace un diagnostico, el cual tiene un costo, y si se quiere continuar con etapas de aseguramiento de vulnerabilidades, se deben considerar costos adicionales, los cuales a veces involucran aparte de la contratación de la empresa, la adquisición de software y hardware.

Es muy importante el tema este de los recursos, porque por ejemplo instituciones públicas grandes cuentan con una unidad de Seguridad Informática independiente. Nosotros en la Contraloría solo contamos con dos personas uno en redes y otro en seguridad, en Wan y Lan y telefonía inalámbrica. Sería deseable contar con una Unidad de Seguridad Informática como un ente separado que dictara las políticas de seguridad a nivel institucional, sin embargo este es un punto que tiene que ver con recursos, personal y eso en época de crisis siempre es complicado.

En cuanto a seguridad física y ambiental, ya hemos establecido perímetros de acceso, en los cuartos de comunicaciones, donde están los switches. Es delicado este punto ya que sin seguridad física cualquier persona podría conectarse a la red.

Esquema de mantenimiento de los equipos, todos los esquemas que requieren para el mantenimiento preventivo y correctivo de los equipos, de los UPS, el aire acondicionado y extintores, todo ese tema está esclarecido en el capítulo de seguridad física y ambiental.

En el tema de comunicaciones y operación contamos con aproximadamente 250 procedimientos establecidos. Procedimientos de operación, respaldo y recuperación. Debemos llegar a contar con manuales autosuficientes, es decir que cualquier persona con conocimiento básico en el tema, pueda entenderlos y aplicarlos.

Dentro del sistema de contingencias, lo que hicimos fue definir los servicios que préstamos. Por ejemplo un sistema de información, el correo electrónico o el uso de Internet son servicios. Cuando hay una eventualidad o una contingencia en un servicio, automáticamente sabemos cuáles son los recursos que están relacionados con éste. Para ponerlo en términos muy simples: en Internet como servicio están relacionados los recursos del cable que conecta con el ISP, el Firewall, el swicht, el router y las líneas internas que van a la computadora del usuario.

Cuando ocurre una eventualidad en el servicio, puede ser producto de una falla en cualquiera de esos puntos. Sí decimos que queremos garantizar el 100% de operación de este servicio, tenemos que garantizar el 100% de todos los recursos relacionados. El sistema de contingencias permite eso, definir a nivel de procedimientos los elementos que se van a activar en el momento en el que ocurre una eventualidad en un servicio.

Se implementó toda la parte que tiene que ver con los certificados digitales, con detectores de intrusos a nivel de redes y a nivel de host, sistemas de seguridad en las conexiones inalámbricas y seguridad en los sistemas de información pública, que es la información que normalmente publicamos y dispositivos para el monitoreo.

Aquí es importantísimo las prácticas que establecimos en los servidores públicos: no pueden haber bases de datos dentro de ellos, ya que cualquier base datos debe estar protegida en la red por medio del firewall institucional. Y los servidores públicos son los más inseguros. No debería haber conexión directa desde Internet hacia las bases de datos institucionales.

Para acceder esa información se hace en dos capas, primero se le solicita al servidor público y éste es quién accede a nuestras bases de datos y le presenta la información al usuario.

Está política nos obligó crear infraestructura y a separar aplicaciones, correo electrónico, el acceso a internet, control de acceso, los procedimientos para la creación de usuarios nuevos, esquemas de autenticación y permisos de los usuarios asignados, esquemas

de los privilegios de los usuarios y todo el tema de certificados digitales que estamos manejando.

Se establecieron esquemas de coordinación a nivel de UTI (Unidad de las tecnologías de la información) para el desarrollo de soluciones tecnológicas, así como coordinación entre la parte de seguridad y la parte de desarrollo, ya que el elemento de seguridad está involucrado en el desarrollo del sistema, en la calidad del software, en la calidad de los participantes del proceso para que no ocurra incidentes de seguridad y en la puesta en marcha del proceso. Se elaboraron procedimientos para la puesta en operación de sistemas, o su mantenimiento, para nuevos requerimientos de TIC y para la separación de los ambientes de desarrollo y de producción.

Sobre el tema de la continuidad de servicios, el marco de seguridad, la puesta en operación del sistema de contingencias se agregó el desarrollo de un sistema de órdenes de servicios (S.O.S), que es un sistema donde todos los usuarios o funcionarios hacen sus reportes de averías.

El sistema S.O.S. se orienta a que cuando algo está afectando a un usuario se localicen soluciones, o para registrar eventos nuevos; el sistema de contingencias se orienta a problemas de carácter masivo y a todo el esquema de manejo de incidentes relacionado.

Actividades permanentes

Estamos desarrollando y haciendo siempre revisión de la aplicación de las políticas, con tecnología, con percepción y análisis de registros. Percepción es ver cómo están funcionando las cosas antes y después de que llegáramos a cambiar algo.La divulgación y sensibilización, que es una de las actividades que más hemos trabajado.

Análisis de brecha del marco de seguridad, definir cuál es la brecha, que es lo que falta para cumplir con el marco de seguridad, ya sea a nivel de tecnología, de procedimientos o de recursos.

Plataforma de soporte

Lo que tenemos a nivel de plataforma de soporte son enrutadores-firewall, firewall especializados a nivel de red y de equipo, enlace

inalámbrico, *anti-relay* de correo, para que no usen nuestros servidores de correo como un relay para enviar *spam* para sitios externosa, *Anti-Spyware-Virus-Phising-Spam*, tenemos también con el proveedor de servicios contratado este nivel de protección, ya que tenemos más de 80.000 correos diarios entrando y los de spam no llegan hasta el usuario final, sin embargo antes del acuerdo que tenemos con el proveedor de servicios no teníamos forma de cómo controlarlos sobre la línea dedicada, ahora el proveedor se encarga de esto, gracias el tipo de tecnología que contratamos con ellos. Esto nos liberó el canal de internet de mucha carga innecesaria.

Certificación de página

Tenemos certificación de página, robot de respaldos, todo el tema de telefonía IP, las redes conmutadas como les decía las redes internas, las inalámbricas, todas contraladas con un Firewall institucional, las redes inalámbricas son internas con certificados digitales y dos redes que son internas con autenticación y una externa que es con control de acceso, para teléfonos y dispositivos móviles.

Tenemos acceso privado a redes de otras instituciones, todo separado por un Firewall institucional y en redes separadas. Tenemos una red insegura, que se orienta a personal que no forma parte de la planilla institucional, pero que labora dentro del campus. Por ejemplo los funcionarios de la Soda o de Servicios Médicos.

Esta red insegura es contralada por el programa de filtro de contenidos por razones obvias de uso: si empiezan a bajar música o bajar vídeos por ahí, nos daría problemas, porque nos estarían comprometiendo el ancho de banda general.

Datos relevantes

Lo que nos reportan los detectores de intrusos: 16 ataques “Altos” por hora, denegación de servicios, ataques de saturación, caída de servicios, 241 ataques “medios”, por ejemplo comunicación por Skype, Messenger, el detector de intrusos esto lo toma como un ataque, lo controla, lo filtra o lo avisa por lo menos. Y 103 ataques “bajos” por ejemplo ataques de reconocimiento de equipos, cuando hay alguien viendo a ver si logra atacar.

Actualmente somos 623 funcionarios. Los oficiales de seguridad y conserjes comparten máquinas y mantenemos más o menos 540 usuarios conectados, de esos como 150 generalmente permanecen conectados inalámbricamente.

Y en proceso están la auditoría de TI, actualización permanente de políticas, el control de acceso a la red NAC que esto es una tecnología que en el momento que alguien se conecte a la red de la institución antes de darle el paso hacia la red interna, le hace toda una verificación de sanidad, esto es un control de: antivirus actualizado, sí tiene las actualizaciones de Microsoft hasta la fecha y un firewall, el revisa esas tres cosas, por lo menos estas tres cosas deben estar instaladas, para nosotros es nuestro esquema de "sanidad", si cumple con eso lo dejamos entrar y si no lo mandamos a una sala de cuarentena y en la sala de cuarentena pueden suceder dos cosas o lo sanamos o le decimos simplemente usted no puede entrar porque su equipo no cumple con los requisitos NAC, esto lo estamos adquiriendo en este año y toda la parte de firma digital que ustedes saben que está en implementación .

Con respecto al software no facturable, nosotros en la Contraloría, empezamos con un proyecto, para ver qué es lo que sucede durante y con la implementación de éste. Además, de que a la dependencia jurídica de contrataciones le están llegando solicitudes de contrataciones para adquisición de software de ofimática con Microsoft y la Contraloría lo que solicita es que se evalúen propuestas alternativas, pudiendo ser de utilidad un proyecto de este tipo para generar un mejor criterio. Iniciamos con la implementación de este tipo de software, apoyándonos en dos compañeros que estaban terminando su maestría en el tecnológico y comenzamos con 25 o 30 personas en la contraloría y por recomendaciones que nosotros consideramos importantes, partimos de cero; es decir, formateamos el equipo.

Partir de cero es todo en ambiente software no facturable: Linux, Open Office completo, a esas 25 personas las capacitamos en Open Office, en Linux y les creamos un ambiente parecido al de Windows en su máquina para que no lo sintieran mucho y el asunto empezó muy bien y hemos mantenido dos compañeros de soporte para que les dieran asistencia durante el proceso y de esos 30 ahora nos quedan 8.

El problema que hemos tenido es la no compatibilidad del *Power Poin*t con su símil en *Open Office* y lo otro; que ya lo sabíamos, a nivel de *Excel no existe compatibilidad en un 100%* con lo que son macros, prácticamente no es funcional y la otra falla que nos ha dado es que las tablas y este tipo de cosas que se insertan en Word en el traslado de documentos de una persona que tiene *Open Office a Office* y viceversa , se descuadraba la información.

Desde el punto de vista de gestión, el software no facturable se debe evaluar para reducir la factura, evaluando muy bien la compatibilidad de funciones y la estabilidad del producto. Inicialmente teníamos correo ORACLE y decidimos cambiarlo a software no facturable Zimbra, sin embargo, la versión no facturable de ZIMBRA no tiene las funcionalidades de respaldos, ni de recuperación de buzones, dos funcionalidades que sí no se tienen y sucede algo, simplemente se perdió el puesto y entonces como lográbamos que ZIMBRA tuviera esas dos funcionalidades, había que pagar.

Lo no facturable generalmente no cubre todo lo que se necesita, siempre compramos ZIMBRA a un muchísimo mejor precio que otros software disponibles, lo cual es muy importante.

En los servidores nosotros hemos venido trabajando con Linux. Por ejemplo un software para administración de contenidos , le puede costar 15 o 20 mil dólares y existe software para administración de contenidos; muy buenos, que no se facturan.

Respecto al tema de las llaves malla, es un tema muy difícil, nosotros estamos en una constante lucha contra los puntos vulnerables, las llaves son uno de ellos. Ahora hay dos filosofías una es muy restrictiva y es cerrar el uso de éstas al personal, en la mayoría de los seminarios de capacitación en temas de seguridad, la recomendación es cierren el uso de llaves.

Hemos seguido una política de uso masivo de las tecnologías, y si prohibimos el uso de las llaves restringimos las tecnologías, lo que hemos tratado de hacer es instalar medidas de seguridad y software adicional que nos garanticen que si esas llaves tiene algún tipo de contaminación puedan ser contraladas.

Es una lucha constante, porque si hay un virus nuevo el antivirus no lo detecta, el famoso "día cero", es una tarea constante de investigación, el *firewall personal*, las medidas de seguridad, el bloqueo de las máquinas. El asunto es que ya sea con políticas restringidas o sin políticas restringidas, que sean más permisivas el asunto es reforzar la seguridad.

Un alto porcentaje de las políticas las aplicamos a través del Active Director, inclusive las contrataciones de software no facturable entran a través del directorio activo y si no entran por esta vía no se implementan. Casos como el sencillo bloqueador de pantalla cada diez minutos. Por eso los protectores de pantalla a través del Active Director y de las políticas, son muy necesarios, no sólo para la protección de la institución, sino también para la protección del funcionario.

Aquí hay un punto importante con respecto al uso de la tecnología vs. ser un poco más restrictivo, por ejemplo *Youtube*, es un tema importante de discusión, si alguien pasa viendo *Youtube*, oyendo música que no son para nada relacionados con el trabajo, están consumiendo importante ancho de banda sin ser productivo.

Entonces el programa de filtro de contenido los filtra o los empieza a abrir a ciertas personas, luego decidimos bloquearlo, pero en algunos casos estábamos bloqueando información relacionada con el trabajo del funcionario, y esto nos obligó a adquirir tecnología especializada en la administración del ancho de banda, lo que hicimos fue decirle a esta tecnología, se va a usar *Youtube* pero no puede consumir más de tanto ancho de banda. De esa forma no estamos obstruyendo el uso de la tecnología pero sí estamos protegiendo nuestro ancho de banda, para no comprometer aplicaciones básicas de la Contraloría y esto nos ha dado resultado, la gente tiene que competir por el ancho de banda. El punto es controlar, administrar, pero no limitar. Limitar a las nuevas generaciones en materia tecnológica nos parece un error sumamente grave.

En la Contraloría aprovechamos las charlas de inducción y de seguridad para extenderlas a los padres y les damos un software no facturable, se llama K9 que es de la empresa *Blue Coat*. También, comentarles que en la Contraloría se están haciendo audiencias orales cuando

hay alguna apelación, se graban y eso queda como una prueba, es parte de la audiencia. La pregunta es si vamos a tener disponibles esos videos y si lo vamos a tener disponibles nos vamos a convertir en un pequeño *Youtube*, no es nuestro negocio, pero tenemos que entrar a negociar con canales de comunicación grandes, como por ejemplo con *streaming*.

Una de las normas básicas de la Contraloría es la responsabilidad que tienen los usuarios de sacar los respaldos de la información importante y ahí lo que estamos respaldando ellos o nosotros solamente son los documentos que están en proceso, porque los documentos ya emitidos entran al sistema automatizados de gestión de documentos y todos los documentos quedan ahí.

La última capacitación que dimos fue en *PDF Creator* porque todos los documentos que van al sistema de gestión van en PDF y lo otro es que las políticas que la Contraloría dicte lo que busca es no co–administrar, cada institución es libre de decir que es lo mejor para su institución, la Contraloría lo que trata es de no meterse si no de fiscalizar que lo que están haciendo es correcto.

Este es un trabajo que se hace en tres capas, en tres columnas una que para mí es vital la sensibilización, de hecho todas las políticas que hemos implementado han sido posterior a impartir una charla de sensibilización, tratando de no usar un lenguaje técnico.

Lo segundo es incorporar procedimientos paralelos, todo esto del reciclaje de los discos que contábamos es producto de un procedimiento de un documento que está ahí, no es que se nos antoja hacer esto sino que es un procedimiento establecido.

Y lo tercero cuando aplique es el uso de la tecnología, por ejemplo el uso masivo de los correos electrónicos, se les explica que no es conveniente porque saturan los servidores, que cuando no usan copia oculta exponen una cantidad importante de correos a terceras personas y hay una política respecto a eso y sí el software del correo lo permite, en este caso ZIMBRA hay una lista de correos que se llama funcionarios y ese funcionario no puede enviar ese tipo de correos a todos los funciona-

rios aunque esté autorizado, son cosas en donde la tecnología tiene que lidiar con el eslabón más débil de la cadena, el usuario.

Finalmente, puede ser que se asuman ciertas cosas y puede ser que se esté un poco errado, por ejemplo uno cree que las personas que están siendo graduadas en este momento conocen las herramientas básicas de *ofimática* para trabajar, y la responsabilidad en esto la tienen las universidades, por ejemplo la Contraloría no debe capacitar funcionarios en cómo usar *Office*, usted tiene que tenerlo de oficio y a partir de ahí viene todo un proceso de actualización vía capacitación sobre TICs y herramientas avanzadas, pero una persona que va ocupar un puesto donde debe utilizar esto no se le va a capacitar en cosas básicas.

Perfil de los expositores

- **Alfaro Calvo, Francia**
  Psicóloga graduada de la UCR y egresada de la maestría de Tecnología Educativa de la UNED. Es parte de la cooperativa Sulá Batsú en donde trabaja en temas relacionados con el uso social de e-learning y las tecnologías de Información y Comunicación.
- **Avendaño Rivera, Alicia**
  Master en Administración Tecnología de la Información, Universidad Nacional. Maestría en Finanzas Internacionales de la National University-FUNDEPOS. Directora de la Secretaría Técnica de Gobierno Digital. Desarrolló e implementó los proyectos de licencias y pasaportes por medio de las oficinas del Banco de Costa Rica.
- **Baltodano Xatruch, Edgardo**
  Coordinador del área de Gestión de usuarios del Centro de Informática y profesor de la Escuela de Computación e Informática de la Universidad de Costa Rica. Egresado de la carrera de Computación Informática de la UCR. Licenciado de Informática Educativa de la UNED.

- **Barrantes Sliesarieva, Gabriela**
  Directora de la escuela Ciencias de la Computación, de la UCR. Doctora en Ciencias de la Computación, Universidad de Nuevo México. Su investigación doctoral estuvo relacionada con el tema de la seguridad informática. Ha escrito varios artículos sobre el tema.

- **Blanco Incer, Jorge**
  Licenciado en Ingeniería Eléctrica UCR. Postgrado en Arquitectura de Conmutación y Transmisión de Datos, Universidad Politécnica de Madrid. Maestría en Administración de Empresas, Universidad Latina de Costa Rica. Dentro del ICE es el coordinador del área para asegurar la calidad de los servicio de datos a nivel institucional.

- **Calvo Delgado, Jéssica**
  Licenciada en Economía, Master en Administración de Empresas. Desde hace ocho años trabaja en el sector de ciencia y tecnología. Administra la unidad NIC-Internet Costa Rica, de la Academia Nacional de Ciencias el ente responsable del registro y administración de los nombres de dominio bajo el Dominio Superior .cr.

- **Carvajal Pérez, Marvin**
  Director de la Escuela Judicial. Director de la Maestría Hispanoamericana en Justicia Constitucional de la UCR. Doctor en Derecho Constitucional por la Universidad de Sao Paulo, Brasil. Especialista en Derecho Administrativo por la Universidad de Salamanca, España.

- **Cascante Hernández, Denis**
  Licenciado en Ingeniería Informática, Master en Administración de Negocios, obtuvo los Certificado en Ethical Hacker por International Council of E-Commerce consultants, Auditor especializado en Administración de Seguridad de la Información ISO 27001. Asesor de seguridad informática del Tribunal Supremo de Elecciones.

- **Castro Molina, Ana María**

  Ingeniera en Sistemas Informáticos. Licenciada en Desarrollo de Sistemas, con cuatro especialidades en seguridad (Sistemas Operativos, Redes, Sistemas de Gestión de Seguridad Informática, Análisis Forense), 2 Postgrados en Seguridad y Master en Seguridad Informática de la Universidad Oberta de Catalunya Barcelona. Trabaja en Seguridad Informática para la Caja Costarricense de Seguro Social.

- **Castro Zeledón, Jorge**

  Licenciado en Ciencias de la Computación de la UCR. Tiene 10 años de experiencia en temas de infraestructura tecnológica y 8 en el campo de seguridad.Certificado como MCSE y CISSP y en proceso de certificarse como CISA. Laboró en seguridad a clientes de la empresa Hewlett-Packard de Costa Rica.

- **Cerdas Ross, Luis**

  Cuenta con más de 21 años de experiencia en el área del aseguramiento de la información. Fundador de la primera empresa dedicada exclusivamente a la seguridad informática y a la seguridad administrada en Costa Rica. A estado a cargo del diseño de múltiples soluciones y arquitecturas de seguridad para entidades gubernamentales, entidades financieras y empresas privadas. Actualmente es el Director de Operaciones de Seguridad para Managed Security Agency, S.A.

- **Chavarría Cerdas, Johnny**

  Licenciado en Informática con énfasis en Administración de Empresas y Auditor en Informática de la Universidad de Costa Rica. Director de Informática del Registro Nacional. Consultor nacional e internacional en Sistemas de Información.

- **Chinchilla Sandí, Carlos**

  Magistrado Sala Tercera de lo Penal, Corte Suprema de Justicia. Doctor en Derecho Penal por la Universidad Complutense de Madrid. Especialista nacional e internacional en temas sobre criminalidad económica, crimen organizado, delitos informáticos, corrupción y enriquecimiento ilícito.

- **Chirino Sánchez, Alfredo**

  Doctor en Derecho. Catedrático de la Facultad de Derecho de la UCR. Juez Regional de Casación de San José, asesor en soporte legal en varios gobiernos. Profesor de diversas materias de postgrados en Centroamérica. Autor de varias obras sobre derecho penal, procesal y constitucional. Especialista en el tema de protección de datos personales.

- **Cordero Rojas, Luis Roberto**

  Abogado con más de 10 años de experiencia como consultor externo en temas de Tecnología. Director de proyectos de la empresa costarricense, Identiga Karto, dedicada a temas de seguridad informática, firma digital, encripción y protección de la información.

- **Cuadra Chavarría, Cilliam**

  Ingeniero de Sistemas por el Instituto Tecnológico de Costa Rica y Máster por el Programa de Maestría Profesional en Auditoría de Tecnologías de Información de la Universidad de Costa Rica. Especialista en Control y Seguridad de la Tecnología de Información. Labora para el Banco Nacional de Costa Rica, donde coordina Unidad de Seguridad de la información.

- **Elizondo Giangiulio, Richard**

  Ingeniero de soporte del Departamento de Sistemas de RACSA, encargado del diseño, implementación, aseguramiento y operación de infraestructura de servicios. Máster en Telemática del Instituto Tecnológico de Costa Rica. Realizó estudios especializados en administración de servidores, redes, sistemas operativos y seguridad de la información.

- **Espinoza Sánchez, Luis Diego**

  Especialista en tecnologías de información y comunicación con amplia experiencia y conocimiento en tecnologías de Internet. Colaboró con en el grupo de trabajo que estableció las primeras conexiones a Internet en el país. Como asesor del Ministerio de Ciencia y Tecnología, coordinó la implementación del plan piloto de la Red Internet Avanzada del ICE y realizo importantes aportes a su diseño.

- **Esquivel Gutiérrez, Walter**

  Graduado en Agroindustria. Master en Evaluación de Programas y Proyectos de Desarrollo de la UCR. Desarrolló su tesis en el área Adolescencia y Ciberespacio. Cursa la maestría virtual en Ciencias de la Información del Tecnológico de Monterrey. Es coordinador de la Unidad de Iniciativas Tecnológicas de la Fundación Paniamor. Tiene 12 años de experiencia en la gestión de proyectos sociales.

- **Esquivel Herrera, Luis Diego**

  Ingeniero en Computación con formación académica en el Instituto Tecnológico de Costa Rica y la Universidad Internacional de las Américas. Gerente de Producto de las líneas de Cliente e Information Worker para la subsidiaria de Microsoft Costa Rica.

- **Gamboa Sánchez, Celso**

  Abogado, criminólogo. Fiscal Adjunto en San José, Alajuela y actualmente en Limón. Coordinador de la Unidad Especializada en Fraudes. Jefe del equipo de respuesta para incidentes de seguridad cibernética en Costa Rica. Profesor de maestría en la cátedra de Delitos Informáticos en la Universidad Autónoma de Monterrey.

- **García Rojas, Georgina**

  Abogada y Notaria, Master en Propiedad Intelectual. Profesora en el Sistema de Estudios de Postgrado -Facultad de Derecho de la UCR. Participó en la Academia de la Organización Mundial de Propiedad Intelectual para países de habla hispana y lusófona.

- **Garro Arroyo, Miguel**

  Más de 8 años de experiencia en el campo de la Seguridad de la Información. Certificado en Microsoft Certified Systems Engineer +Security, Certified Ethical Hacker, Cisco Certified Network Associate y Certified Information Security Manager. Labora en el área de preventa y diseño de redes en ITS InfoComunicación S.A.

- **Grillo Rivera, Milena**

  Egresada en Derecho y Master en estudios de la Violencia Familiar y Social. Directora Ejecutiva de la Fundación Paniamor, de Costa Rica, desde 1989. Consultora en derechos humanos de la niñez y la adolescencia; la violencia interpersonal y social; la pobreza y la exclusión social; la incidencia política y la movilización social para agencias especializadas. Miembro del Consejo Consultivo del Programa Estado de la Nación desde el año 2000. Miembro del Proyecto Estado de la Educación a partir del 2007, ambas iniciativas del Consejo Nacional de Rectores (CONARE).

- **Gutiérrez Gutiérrez, Joaquín**

  Licenciado en Ingeniería de Sistemas Universidad, Latina de Costa Rica. Oficial de Seguridad en Tecnologías de Información para la Contraloría General de la República. Fue consultor en el proyecto de Gerencia Informática del PNUD. Profesor de Ingeniería de sistemas de la Universidad Latina de Costa Rica.

- **Hess Araya, Christian**

  Licenciado en Derecho y Máster en Informática. Letrado de la Sala Constitucional de la Corte Suprema de Justicia de Costa Rica. Juez del Tribunal Contencioso Administrativo y Civil de Hacienda. Es "senior member" de la Association for Computing Machinery (ACM) de Estados Unidos.

- **Jaikel Chacón, Alvaro**

  Master en Ciencias de la Computación con especialización en sistemas gerenciales del Instituto Tecnológico de Costa Rica. Socio fundador, presidente, asesor y consultor principal en Gobierno Corporativo, Gestión Integrada del Riesgo, Continuidad y Estrategia de Negocio, del Grupo Gestor Cumbres, Presidente de Asociación Costarricense de Auditores en Informática, ACAI.

- **Lewis Hernández, Erick**

  Jefe de la Sección de Delitos Informáticos del Organismo de Investigación Judicial, profesional en informática, con más de 10 años de experiencia en la investigación informática e informática forense.

- **Malavassi Calvo, Federico**

  Abogado y Notario, graduado en la UCR con énfasis en Derecho Público. Catedrático de la Universidad Autónoma de Centro América. Diputado y vicepresidente de la Asamblea Legislativa (2002-2006). Expresidente de ANFE (Asociación Nacional de Fomento Económico). Abogado de la empresa DATUM.

- **Melegatti Sarlo, Carlos**

  Subgerente General del Banco Central de Costa Rica. Es Ingeniero en Computación y Máster en Finanzas. Coordina y apoya la puesta en marcha del proyecto de la "Firma Digital Certificada" para el sector financiero.

- **Mora Fernández, Mauricio**

  Profesor e investigador de la Escuela Centroamericana de Geología de la UCR. Es Licenciado en Geología de la Universidad de Costa Rica. Estudios de volcanología en la Universidad Blaise Pascal de Clermont Ferrand, Francia, y el doctorado en Geofísica en la Universidad de Saboya de ese mismo país. Director del Programa de Posgrado en Geología y Coordinador de la Red Sismológica Nacional (RSN: UCR-ICE).

- **Mora Mora, Luis Paulino**

  Presidente de la Corte Suprema de Justicia. Ex Ministro de Justicia y Gracia. Fue Director del Área de Asistencia Técnica del Instituto Latinoamericano de las Naciones Unidas para el Delito (ILANUD). Magistrado de la Sala Constitucional. Autor de numerosos artículos sobre temas penales. Ha participado en múltiples actividades de capacitación y en la redacción de importantes proyectos de ley. Graduado en Derecho UCR.

- **Ramírez López, Rafael**

  Licenciado en Computación e Informática y en Contaduría Pública con énfasis en Administración y Finanzas. Master en Administración con énfasis en Auditoria Informática. Jefe del Departamento de Tecnología de la Información y Comunicaciones del Poder Judicial.

- **Rodríguez Rojas, Oldemar**
  Doctor en Informática del U.F.R. Matemáticas de la Decisión, Universidad de París IX–Dauphine, Francia. Miembro del Consejo Universitario de la Universidad de Costa Rica. Obtuvo la Medalla de Oro al Inventor Destacado del Año 2004 otorgado por la OMPI por su trabajo "Symbolic Personal Vector to detect frauds in credit cards".

- **Rojas Rivero, Adriana**
  Abogada de la Asociación Nacional de Consumidores Libres. Litiga en procesos colectivos en defensa de derechos de los usuarios de servicios financieros. Profesora universitaria y conferencista en el ámbito nacional e internacional.

- **Salas Ruiz, Francisco**
  Licenciado en Derecho por la UCR. Magíster en Derecho de la Informática y las Telecomunicaciones - Universidad de Chile. Procurador en Derecho Informático e Informática Jurídica. Director del Sistema Nacional de Legislación Vigente (SINALEVI).

- **Sánchez Castillo, Sergio**
  Licenciado en Geografía Física de la Escuela de Geografía de la Universidad Nacional. Tiene postgrado en Planificación del Paisaje Ecológico en Berlín, Alemania. Profesor e investigador en la Escuela de Ciencias Geográficas de la UNA. Es geógrafo del Sistema de Información para Emergencias, departamento de Prevención y Mitigación de la CNE.

- **Severino, Nicolás**
  Responsable de las operaciones de Ingeniería (preventa) de Symantec para el Norte de Latinoamérica, región que comprende los distritos de Caribe, Centroamérica, Andino y Venezuela, tiene más de quince años de experiencia en la industria de las tecnologías de información. Especialista en temas de seguridad de la información, infraestructura y networking.

- **Solano González, Jonathan**

  Especialista en telecomunicaciones, consultor en seguridad informática de ITS InfoComunicación. Realizó estudios en la Escuela de Ingeniería Electrónica del Tecnológico de Costa Rica, cuenta con 16 años de experiencia en temas relacionados con la seguridad.

- **Solís Solís, Oscar**

  Licenciado en Derecho. Director de la Dirección de Certificadores de Firma Digital y preside el Comité Asesor de Políticas que brinda apoyo a la Dirección de Certificadores de Firma Digital. Colaboró en la redacción de la Ley de Certificados, Firmas Digitales y Documentos Electrónicos, su Reglamento, el Decreto Ejecutivo 34890-MICIT.

- **Villalobos Salas, Jairo**

  Ingeniero de Sistemas, graduado de la Universidad Nacional. Es Chief Operations Officer de SmartSoft . Posee más de 8 años de experiencia en la implementación de sistemas enfocados en la prevención de fraude y lavado de dinero en instituciones financieras de 14 países de América.