JORNADAS DE INVESTIGACIÓN
Ciberseguridad y resiliencia digital en tiempos contemporáneos

10, 11 y 12 de noviembre, 2025

I. Introducción y justificación

La creciente integración de las tecnologías de la información y comunicación (TIC) en los distintos sectores productivos ha propiciado su digitalización y la aparición cada vez más constante, de plataformas, sitios web, aplicaciones y todo tipo de herramientas que han sido incorporadas en una amplia gama de actividades. Esto ha innovado la forma como se produce y modernizado la prestación de los servicios públicos por parte de los Estados; además, está transformando las finanzas, las comunicaciones, la salud y los negocios.

Aunado a ello, estas transformaciones han estimulado el rápido crecimiento del sector de las tecnologías de la información (TI), provocando que este crezca dos veces más rápido que la economía global (Banco Mundial, 2024).

Por lo anterior, es de esperar que esta tendencia hacia la digitalización continúe durante las próximas décadas y es muy posible que se acreciente, con la llegada e integración paulatina de adopción de tecnologías emergentes como la inteligencia artificial (IA) y el Internet de las Cosas (IoT), entre otras. Si bien esto indica que las tecnologías digitales se han convertido en un activo clave para potenciar mayor desarrollo económico y elevar la competitividad de los países; también avizora un futuro más digital en el que habrá mayor dependencia hacia las TIC y las infraestructuras digitales. Sin embargo, conforme se incremente la interconexión entre las empresas, las redes, las aplicaciones y los datos, surge una preocupación esencial sobre la seguridad y la resiliencia que poseen las infraestructuras digitales.

Esta preocupación no es para menos pues durante el 2022, se identificaron un total de 493,33 millones de ataques de ransomware a nivel mundial; mientras que, en el 2023, se estima que se produjo un promedio de 2 244 ciberataques por día (Kolesnikov, 2025). Generalmente, estos ataques son realizados con el fin de acceder de forma no autorizada a sistemas informáticos para robar, manipular o eliminar información sensible; así como para extorsionar a las organizaciones e interrumpir sus operaciones (Akamai Technologies, 2025). Aunado a ello, el *Informe Panorama Global de Ciberseguridad* publicado por el Foro Económico Mundial (FEM) en el 2025, indica que el ciberespacio está complejizándose por factores como la incertidumbre geopolítica, la creciente desigualdad cibernética y la sofisticación de la ciberamenazas.

La rápida evolución tecnológica está provocando nuevas brechas de seguridad, que pueden ser aprovechadas por los ciberdelincuentes. Particularmente, el desarrollo de la inteligencia artificial generativa está potenciado las capacidades de los cibercriminales para escalar los ataques basados en la ingeniería social, lo que les permite alcanzar mayor precisión y escalabilidad (Foro Económico Mundial, [FEM], 2025). De igual modo, la alta rentabilidad y los bajos costos operativos hacen que estas actividades ilícitas resulten

sumamente atractivas, lo que ha contribuido a su rápida expansión. Por todo esto, se cree que el ritmo estos ataques continúe incrementándose.

Ante esto, se ha reforzado la necesidad de proteger los recursos digitales ante potenciales eventos que puedan vulnerarlos, ya que estos no sólo provocan pérdidas económicas y de información, sino que también afectan la imagen de las organizaciones e instituciones afectadas (Lindemulder & Kosinski, 2024). Es en este contexto, que la ciberseguridad ha cobrado especial importancia como un medio para proteger las redes, los equipos, los datos, los sistemas críticos y la información de potenciales amenazas digitales (Amazon Web Services, [AWS], 2024) y con este propósito, se establecen políticas y se usan tecnologías para prevenir, atender, gestionar y mitigar los ciberataques. En consecuencia, hoy la ciberseguridad se considera como un componente estratégico para las organizaciones, sin embargo, su utilidad no acaba aquí pues para los Estados representa un medio para salvaguardar sus infraestructuras críticas, lo que puede llegar a incidir en la estabilidad democrática de los países (Organización de Estados Americanos [OEA], 2023).

Por otro lado, debe subrayarse que el desarrollo de capacidades en ciberseguridad se alinea con las prioridades establecidas en los Objetivos de Desarrollo Sostenible (ODS), en particular el ODS 9 (Industria, innovación e infraestructura) y el ODS 16 (Paz, justicia e instituciones sólidas), al reconocer que la protección de la infraestructura digital es condición indispensable para el ejercicio pleno de derechos, la confianza ciudadana en el Estado y la competitividad de las economías digitales emergentes.

La importancia otorgada a la ciberseguridad también ha llevado a la creación de regulaciones y estándares específicos por parte de los Estados. Por ejemplo, desde el 2022 la Unión Europea (UE) adoptó la Directiva (UE) 2022/2555 (*relativa a las medidas destinadas a garantizar un nivel común de ciberseguridad en toda la Unión Europea*) con el fin de exigirle a los Estados miembro para que "refuercen las capacidades de ciberseguridad e introduzcan medidas de gestión de riesgos de ciberseguridad y notificaciones en sectores críticos[1], junto con normas relativas a la cooperación, el

[1] Como las telecomunicaciones, la salud, la energía y el transporte.

intercambio de información, la supervisión y la ejecución"(Unión Europea, [UE], 2025, párr.1). Por su parte, los Estados Unidos a través del Instituto Nacional de Estándares y Tecnología (NIST)[2] cuenta con el Marco de Ciberseguridad del NIST (CSF del NIST), una herramienta que establece "estándares, pautas y mejores prácticas que ayudan a las organizaciones a mejorar su gestión de riesgos de ciberseguridad" (IBM, s.f., párr.2).

Por su parte, en el caso de Costa Rica, el país ha realizado diversos esfuerzos para fortalecer las capacidades de prevención, gestión y atención de incidentes, mediante la creación del Centro de Respuesta a Incidentes de Ciberseguridad (CSIRT-CR), la promoción de la Estrategia Nacional de Ciberseguridad (una primera publicada en 2017 y actualizada en el 2023), la emisión del Protocolo de Gestión de Incidentes de Ciberseguridad y la creación del Clúster Cybersec Costa Rica, entre otros. A pesar de la trascendencia que han tenido estos valiosos esfuerzos, datos de la Contraloría General de la República (CGR) revelan que menos del 50 % de las instituciones públicas han implementado políticas de seguridad de la información y únicamente un 54 % cuenta con protocolos de atención a incidentes (Contraloría General de la República, [CGR], 2025). Esto significa que una parte sustancial del aparato estatal carece de mecanismos mínimos para enfrentar ataques que ya no son hipotéticos, sino una realidad que afecta directamente la provisión de servicios públicos esenciales.

El panorama se agrava por la incidencia de ciberataques de alto impacto en los últimos años, como los perpetrados contra la Caja Costarricense de Seguro Social (CCSS) en 2022, y más recientemente contra la Dirección General de Migración y Extranjería (DGME) en 2024, que paralizaron servicios críticos e incluso expusieron datos sensibles de la ciudadanía (LabCIBE, 2024). Dichos episodios evidencian que el país enfrenta amenazas persistentes avanzadas (APT, por sus siglas en inglés), ransomware y ataques de denegación de servicio distribuido (DDoS), modalidades que requieren tanto resiliencia tecnológica como capacidades humanas especializadas. De acuerdo con La República (2024), Costa Rica registró más de 1,6 millones de ciberamenazas en un año, lo que la coloca como un objetivo reiterado en la región.

[2] Agencia federal estadounidense dedicada a desarrollar estudios y a crear normativa y estándares técnicos que orientan el desarrollo de diversas tecnologías.

Estas circunstancias plantean la necesidad de cerrar brechas y a mejorar las capacidades nacionales en ciberseguridad, para lo cual resulta indispensable que se articule un ecosistema que sea "seguro, resiliente e inclusivo, fundamentado en cinco pilares: protección, gobernanza, normativa, educación y cooperación internacional" (Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, [Micitt], 2023, p.4).

En este contexto, el Programa Sociedad de la Información y el Conocimiento (Prosic) ha decidido enfocar sus Jornadas de Análisis e Investigación 2025 al tema de la ciberseguridad, en respuesta a la confluencia de factores técnicos, políticos y estratégicos que hacen de esta temática una prioridad para los Estados. Desde esta perspectiva, las *Jornadas de Investigación "Ciberseguridad y resiliencia digital tiempos contemporáneos"* pretenden promover un espacio de diálogo intersectorial y multidisciplinario que propicie la reflexión crítica sobre los desafíos que enfrentan los Estados, las organizaciones y las personas frente a la creciente digitalización, con el fin de sensibilizar y fortalecer las capacidades necesarias para proteger las infraestructuras digitales y promover una cultura de ciberseguridad.

II. Objetivos

General

Promover un espacio de diálogo intersectorial y multidisciplinario que propicie la reflexión crítica sobre los desafíos que enfrentan los Estados, las organizaciones y las personas frente a la creciente digitalización, con el fin de sensibilizar y fortalecer las capacidades necesarias para proteger las infraestructuras digitales y promover una cultura de ciberseguridad.

Específicos

1. Presentar el origen, los fundamentos conceptuales y el contexto internacional actual de la ciberseguridad, destacando las tendencias y los cambios generados en la seguridad de los Estados y las organizaciones.

2. Examinar las transformaciones, los desafíos y las oportunidades generadas por las tecnologías emergentes (inteligencia artificial, blockchain, Internet de las Cosas) en los modelos de seguridad digital.

3. Compartir experiencias y buenas prácticas nacionales e internacionales para la protección de infraestructuras críticas, la gestión de incidentes y la ciberresiliencia organizacional.

4. Identificar estrategias, recomendaciones y buenas prácticas para fortalecer la alfabetización digital, la sensibilización ciudadana y el desarrollo de competencias técnicas ante los riesgos del entorno digital.

5. Analizar los esfuerzos nacionales en materia de ciberseguridad para identificar fortalezas, debilidades y oportunidades de mejora.

III. Metodología

Para llevar a cabo las Jornadas de Investigación *"Ciberseguridad y resiliencia digital en los tiempos contemporáneos"* se desarrollará un evento virtual, el cual será integrado por un conjunto de mesas temáticas definidas con base a los objetivos específicos de las Jornadas. A partir de esto, las intervenciones serán orientadas a 5 temas principales: conceptos básicos, el contexto internacional y la importancia de la ciberseguridad; el impacto de las tecnologías emergentes en las ciberamenazas e implicaciones para la seguridad digital; estrategias para la ciberresiliencia; alfabetización digital enfocada en la ciberseguridad; y esfuerzos realizados en Costa Rica en materia de ciberseguridad. De ese modo, en las Jornadas de Investigación se abordarán las siguientes mesas temáticas:

MESA 1: INTRODUCCIÓN A LA CIBERSEGURIDAD Y LA SEGURIDAD DIGITAL

MESA 2: TECNOLOGÍAS EMERGENTES Y CIBERSEGURIDAD

MESA 3: CIBERRESILIENCIA Y GESTIÓN DE RIESGOS

MESA 4: ALFABETIZACIÓN DIGITAL Y CULTURA DE CIBERSEGURIDAD

MESA 5: ESFUERZOS NACIONALES EN CIBERSEGURIDAD

En línea con lo esbozado previamente, cada mesa temática será integrada por 3 a 5 personas expertas nacionales e internacionales, las cuales presentarán ponencias breves (15 minutos) sobre tópicos específicos de ciberseguridad. Adicionalmente, cada mesa será acompañada por una persona moderadora que se encargará de presentar a cada panelista, así como de controlar el tiempo y realizar las preguntas del público a las y los expositores. Al finalizar las participaciones de las y los panelistas, se dispondrá de un espacio de 15-20 minutos para abordar las preguntas y consultas del público.

Complementariamente, el evento también contará con una conferencia inaugural y otra de cierre para abordar contenidos de alta especialización, a los cuales se les otorgará mayor tiempo de exposición. Debe aclararse que, considerando el número de mesas temáticas y las conferencias, se ha considerado pertinente que las Jornadas sean realizadas durante tres días consecutivos en el horario de 8:30 a.m. a 12:00 p.m.

Para la selección de las y los ponentes se realizará un mapeo preliminar de personas expertas en diversos tópicos, quiénes serán contactadas para hacerles llegar una invitación formal por vía electrónica (en la que se detallarán las condiciones de participación y otros aspectos logísticos relevantes). Al confirmarse las participaciones, a cada ponente le será solicitado el envío de una biografía corta (de 1-2 párrafos), una ponencia escrita y el material audiovisual de apoyo que utilizarán para la presentación durante las jornadas.

Debido a que las Jornadas serán efectuadas de manera virtual y remota, se utilizará la plataforma Zoom para desarrollarlas. Además, se habilitará un formulario de inscripción en el que el público interesado podrá registrarse para obtener los enlaces de acceso a la actividad. Finalmente, debe señalarse que quienes asistan a los tres días del evento y se

registren en las listas de asistencia de cada día, se les entregará un certificado de asistencia.

IV. Medio para realizar las Jornadas de Investigación

Las Jornadas de Investigación *"Ciberseguridad y resiliencia digital tiempos contemporáneos"* serán realizadas el 10, 11 y 12 de noviembre del 2025 en horario de 9:00 a.m a 12:00 p.m. a través de la plataforma ZOOM. A este efecto, se habilitará un formulario de inscripción (en Google forms) en el que el público interesado podrá registrarse para obtener los links de acceso a la actividad.

V. Información de contacto

Si necesita cualquier otra información, por favor comuníquese con el equipo organizador del evento al teléfono +506 2253-6491 o escriba a los correos electrónicos prosic@ucr.ac.cr o valeria.castro@ucr.ac.cr

Referencias

Akamai Technologies. (2025). ¿Qué es la ciberseguridad? ¿Qué es la ciberseguridad o seguridad cibernética? | Akamai

Amazon Web Services. (2024). ¿Qué es la ciberseguridad? ¿Qué es la ciberseguridad? - Explicación de la ciberseguridad - AWS

Banco Mundial. (2024). La digitalización mundial en 10 gráficos. Banco Mundial. La digitalización mundial en 10 gráficos

Contraloría General de la República. (2025). Índice de Capacidad de Gestión de Tecnologías de Información (ICGTI) 2025 [Instrumento de evaluación institucional]. Sitio web de la Contraloría General de la República. Recuperado de https://sites.google.com/cgr.go.cr/icgti

Foro Económico Mundial. (2025a). Global Cybersecurity Outlook 2025 Insight Report. FEM. WEF_Global_Cybersecurity_Outlook_2025.pdf

IBM. (s.f.). ¿Qué es el marco de ciberseguridad del NIST? IBM.

Kolesnikov, N. (5 de octubre de 2024). 50 Estadísticas Clave de Ciberseguridad para Septiembre de 2025. En: Techopedia. 50 Estadísticas Ciberseguridad y Ataques Cibernéticos 2025

LabCIBE, Universidad Nacional. (2024, mayo 12). Ransomware y fuga de información: principales amenazas en ciberseguridad. UNA Comunica. https://www.unacomunica.una.ac.cr/index.php/mayo-2025/6085-ransomware-y-fuga-de-informacion-principales-amenazas-en-ciberseguridad

La República. (2024, diciembre 21). Costa Rica en la mira: más de 1,6 millones de ciberamenazas detectadas en un año. La República. https://www.larepublica.net/noticia/costa-rica-en-la-mira-mas-de-16-millones-de-ciberamenazas-detectadas-en-un-ano

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones. (2023). Estrategia Nacional de Ciberseguridad 2023-2027. MICITT. https://micitt.go.cr/el-sector-informa/micitt-presenta-la-estrategia-nacional-de-ciberseguridad-2023-2027

Organización de Estados Americanos. (2023). Ciberseguridad en América Latina y el Caribe: retos y perspectivas. Secretaría de Seguridad Multidimensional.

Unión Europea. (2025). Ciberseguridad de las redes y sistemas de información. Euro-Lex. Directiva (UE) 2022/2555 del Parlamento Europeo y del Consej...

Unión Internacional de Telecomunicaciones. (2021). Global Cybersecurity Index 2021. UIT.

World Economic Forum. (2024). Global cybersecurity outlook 2025. https://es.weforum.org/publications/global-cybersecurity-outlook-2025/