LABORATORIO DE I + D + i
LABCIBE
EN CIBERSEGURIDAD

50 AÑOS CONARE
CONSEJO NACIONAL DE RECTORES

UNA UNIVERSIDAD NACIONAL COSTA RICA
SEDE REGIONAL CHOROTEGA

Hallazgos del informe “Estado de la Ciberseguridad en Costa Rica 2024, desde el enfoque Jurídico, Investigación y Desarrollo" LabCIBE UNA 2025.

Ing. Raymond A. Pérez Meza. M.Sc.

Académico Investigador LabCIBE.

Agenda

- Sobre LabCIBE – Universidad Nacional.
- Situación jurídica de la ciberseguridad nacional.
- Investigación y desarrollo de la ciberseguridad.
- Diagnóstico de la situación de la ciberseguridad en Costa Rica.
- Conclusiones.

UNA

¿Qué es el LabCIBE?

- El Laboratorio de I+D+i en Ciberseguridad tiene como misión impulsar proyectos de investigación, desarrollo e innovación en Ciberseguridad, mediante recurso humano especializado y tecnología científica en la Universidad Nacional (UNA), en aspectos relacionados con ciberseguridad, la atención a incidentes, la preservación de la privacidad y construcción de herramientas de software.

Estado de la ciberseguridad en Costa Rica 2024.

VICERRECTORÍA DE INVESTIGACIÓN
UNIVERSIDAD NACIONAL

LABORATORIO DE I + D + i
LABCIBE
EN CIBERSEGURIDAD

UNA
UNIVERSIDAD NACIONAL
COSTA RICA

¿Qué es la ciberseguridad?

- La ciberseguridad constituye un elemento fundamental dentro del marco más amplio de la seguridad de la información. Se define como el conjunto de medidas y prácticas destinadas a proteger los activos de información digital contra amenazas que afectan a datos procesados, almacenados y transmitidos a través de sistemas interconectados.
- A diferencia de la seguridad de la información, que abarca todos los formatos de datos, la ciberseguridad se especializa específicamente en la protección de activos digitales, incluyendo hardware de red, software y la información que fluye a través de los sistemas informáticos (ISACA, 2021).

¿Qué son las amenazas informáticas?

- Virus y malware.
- Phishing.
- Ataque de fuerza bruta.
- Ataques DDoS.
- Exploits.
- Intercepciones man-in-the-middle.

Marco regulatorio de la ciberseguridad en Costa Rica.

VICERRECTORÍA DE INVESTIGACIÓN
UNIVERSIDAD NACIONAL

LABORATORIO DE I + D + i
LABCIBE
EN CIBERSEGURIDAD

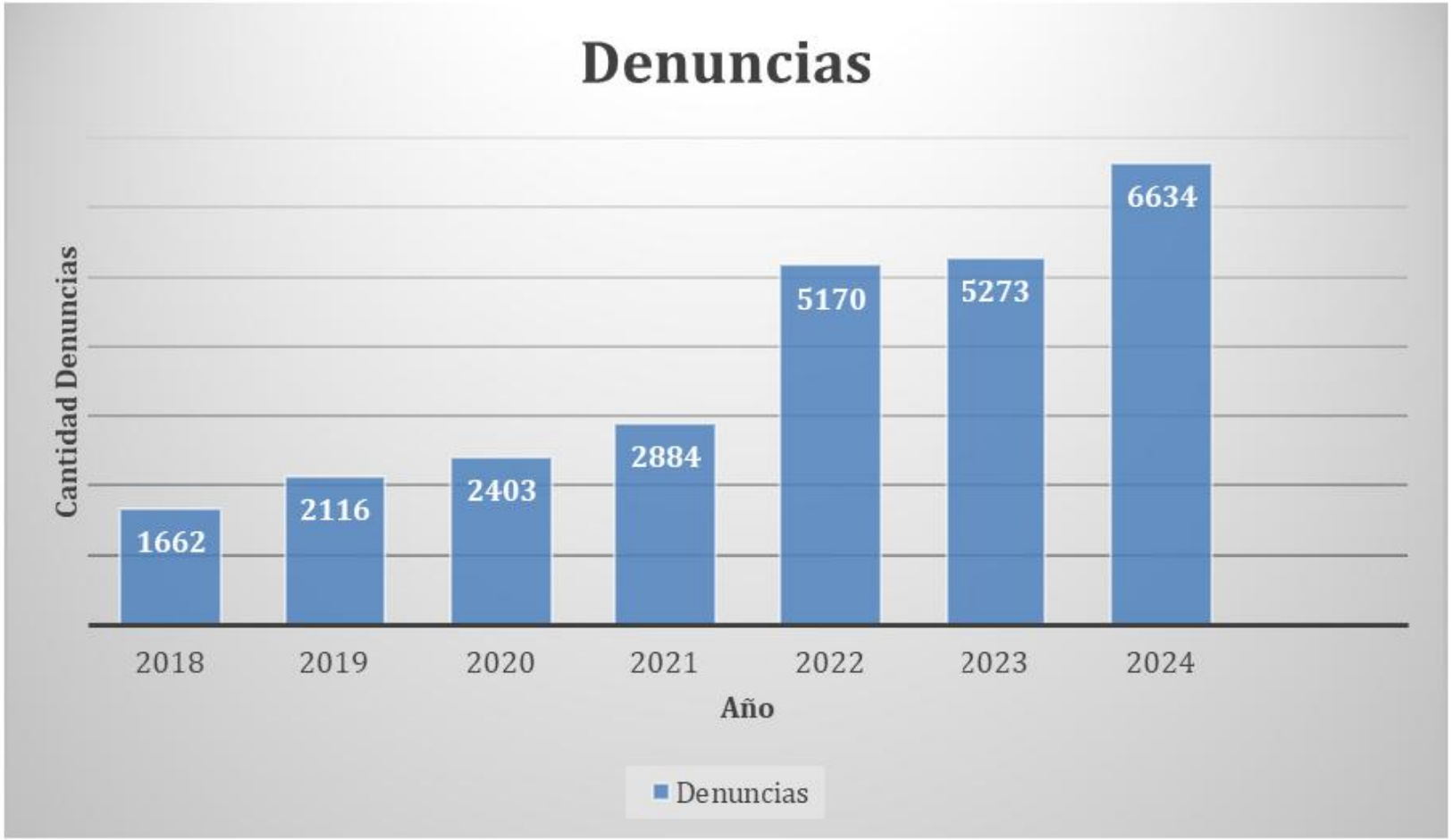
UNA
UNIVERSIDAD NACIONAL
COSTA RICA

Tabla 1. Cantidad de denuncias por Delitos Informáticos, según año, período comprendido del 01/01/2018 hasta el 15/10/2024

Año	Totales
2018	1662
2019	2116
2020	2403
2021	2884
2022	5170
2023	5273
2024*	6634
Total:	26142

Fuente: Unidad de Análisis Criminal OIJ 2024

Gráfico 1. Denuncias por Delitos Informáticos, según año. Período comprendido del 1/01/2018 hasta 15/10/2024



Fuente: Unidad de Análisis Criminal OIJ 2024

Tabla 2. Cantidad de denuncias por Delitos Informáticos, según Delito y Año. Período comprendido del 01/01/2018 hasta el 31/10/2024

	AÑO							
Delito	**2018**	**2019**	**2020**	**2021**	**2022**	**2023**	**2024**	**Totales**
ESTAFA INFORMATICA	398	645	926	935	3112	3272	4840	14128
SUPLANTACION DE IDENTIDAD	399	645	796	1032	845	1195	1726	6638
OTRO O INDETERMINADO	520	483	137	216	207	281	201	2045
DIFUSION DE INFORMACION FALSA	50	103	119	162	217	143	131	925
SUPLANTACION DE PAGINAS ELECTRONICAS	88	32	36	104	285	64	130	739
ESPIONAJE INFORMATICO	32	51	122	131	135	137	79	687
FACILITACION DE DELITO INFORMATICO	68	47	51	108	166	54	66	560
SEDUCCION O ENCUENTRO CON MENORES POR MEDIOS ELECTRONICOS	54	55	52	65	84	54	74	438
INSTALACION O PROPAGACION DE PROGRAMAS INFORMATICOS MALICIOSOS	4	6	88	74	47	18	15	252
SABOTAJE INFORMATICO	17	15	31	26	22	25	11	147
DAÑO INFORMATICO	12	10	19	18	18	9	5	91
Totales	**1642**	**2092**	**2377**	**2871**	**5138**	**5252**	**7278**	**26650**

Fuente: Unidad de Análisis Criminal OIJ 2024

Leyes

- Ley de la Administración Financiera de la República y Presupuestos Públicos N.º 8131.
- Ley de Certificados, Firmas Digitales y Documentos Electrónicos N.º 8454 y su Reglamentos.
- Ley de protección de la niñez y la adolescencia frente al contenido nocivo de internet y otros medios electrónicos N° 8934.
- Ley de protección de la persona frente al tratamiento de sus datos personales N.º 8968 y su Reglamento.
- Código Penal Ley N° 9048: Reforma de varios artículos y modificación de la sección VIII, denominada delitos informáticos y conexos, del título VII del Código Penal.
- Adhesión de la República de Costa Rica al Convenio de Europa sobre Ciberdelincuencia.

Decretos

- Reglamento para la Protección de los Programas de Cómputo en los Ministerios e Instituciones Adscritas al Gobierno Central - N° 37549-JP.
- Creación Comisión Internet Costa Rica, CI-CR.
- Creación de la Comisión Nacional de Seguridad En Línea N.º 36274-MICIT.
- Creación del "Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR)" N.º 37052-MICIT.
- Directriz N° 133-mp-micitt dirigida a la administración pública central y descentralizada sobre las mejoras en materia de ciberseguridad para el sector público del estado.

Decretos

- Decreto N° 46 H-MICITT “Instituciones del sector público privilegiarán la adquisición de soluciones de cómputo en la nube sobre otro tipo de infraestructura”.
- Directriz N.° 036-MTSS-MICITT, "Implementación de accesibilidad de la red de los sitios del sector público“.
- Decreto N.º 44196-MSP-MICITT Reglamento sobre medidas de ciberseguridad aplicables a los servicios de telecomunicaciones basados en la tecnología de quinta generación móvil (5g) y superiores.

Estrategia Nacional de Ciberseguridad MICITT 2023-2027

Cuadro 3. Principios y Ejes Transversales de la Estrategia Nacional de Ciberseguridad 2023 - 2027

Principios Rectores	Ejes Transversales
Respeto a los Derechos Humanos y la Privacidad	Alianza público-privada
Enfoque basado en riesgos y resiliencia cibernética	Fortalecimiento del marco legal en ciberseguridad y TIC
Coordinación y corresponsabilidad de múltiples partes interesadas	Convenios Internacionales
Fomento de Cooperación Internacional	Colaboración y coordinación interinstitucional

Fuente: Elaboración propia con base en la Estrategia Nacional de Ciberseguridad, 2023

Estrategia de Transformación Digital 2023 - 2027

Cuadro 4. Principios Rectores y Ejes Estratégicos de la Estrategia de Transformación Digital 2023 - 2027

Principios Rectores	Ejes Estratégicos
Ética Universalidad Desarrollo Humano Creación colaborativa Política Pública basada en Datos Respeto a la Dignidad Humana	Ciudadanía Digital • Firma digital certificada e identidad digital • Servicios Digitales • Habilidades digitales
	Buena Gobernanza • Gobernanza de datos • Interoperabilidad • Actualización de la normativa

Fuente: Elaboración propia con base en la Estrategia de Transformación Digital, 2023

Estrategia Nacional de Inteligencia Artificial 2024 - 2027

Cuadro 5. Principios Rectores y Transversales de la Estrategia Nacional de Inteligencia Artificial 2024 - 2027

Principios Rectores	Principios Transversales
Paz y dignidad humana	Enfoque de género
Supervisión humana	Inclusión y accesibilidad
Transparencia y explicabilidad	Protección de datos, propiedad intelectual y privacidad
Responsabilidad	Promover I+D+I
Sostenibilidad y bienestar	Educación y capacitación
Seguridad y ciberseguridad	

Fuente: Elaboración propia con base en la Estrategia Nacional de Inteligencia Artificial, 2024

- Decreto Ejecutivo N° 44487-MICITT: Lineamientos para la Implementación del Proyecto de Fortalecimiento de las Capacidades en Ciberseguridad del País.
- Marco Normativo de Gobierno y Gestión de las Tecnologías de Información (TI) en Costa Rica.
- Código Nacional de Tecnologías Digitales (N°44507-MICITT).
- Regulación y Normalización de Adquisiciones de Tecnología y/o Desarrollo de Sistemas Informáticos de Apoyo a la Gestión (N°053-H-MICITT).
- Ley Marco de Acceso a la Información Pública (N° 10554).

Investigación y desarrollo de la ciberseguridad.

VICERRECTORÍA DE INVESTIGACIÓN
UNIVERSIDAD NACIONAL

LABORATORIO DE I + D + i
LABCIBE
EN CIBERSEGURIDAD

UNA
UNIVERSIDAD NACIONAL
COSTA RICA

Entidades.

- Cámara de Tecnologías de Información y Comunicación (CAMTIC).
- Cybersec Clúster.

Industria de la Ciberseguridad en Costa Rica.

- Principales servicios que brindan dichas empresas.

- Consultoría en ciberseguridad.
- Servicios administrados de seguridad (MSSP).
- Pruebas de penetración y análisis de vulnerabilidades.
- Cumplimiento normativo y certificaciones.
- Formación y concentración en ciberseguridad.

Ciberseguridad en la academia.

VICERRECTORÍA DE INVESTIGACIÓN
UNIVERSIDAD NACIONAL

LABORATORIO DE I + D + i
LABCIBE
EN CIBERSEGURIDAD

UNA
UNIVERSIDAD NACIONAL
COSTA RICA

Sector Público.

Instituto Tecnológico de Costa Rica (TEC).

- Maestría en Ciberseguridad (énfasis seguridad del software, defensa y ataque de sistemas y gestión de la seguridad de la información).

Universidad de Costa Rica (UCR)

- Incluyen cursos en plan de Ciencias de Computación e informática.

Universidad Nacional (UNA)

- Se prevé para el 2025 la Maestría en Ciberseguridad Industrial en la Sede Regional Chorotega, impulsada por el LabCIBE.

Universidad Técnica Nacional (UTN)

- Incluye cursos en el plan Ingeniería en Tecnologías de Información.

Universidad Estatal a Distancia (UNED)

- Incluye cursos en su plan de Ingeniería Informática.

Sector Privado.

Universidad Cenfotec.

- Maestría y Técnico en Ciberseguridad.

Universidad Latina de Costa Rica.

- Licenciatura en Seguridad Informática.

Universae

- Licenciatura en Ingeniería en Ciberseguridad.

Universidad Fidélitas

- Bachillerato y Técnico en Ingeniería Seguridad Informática.

Sector Privado.

Universidad La Salle.

- Técnico en Ciberseguridad.

Universidad Castro Carazo.

- Técnico en Ciberseguridad 2.0.

Lead University

- Técnico especializado en Ciberseguridad.

Ministerio de Educación Pública.

Técnico en Ciberseguridad.

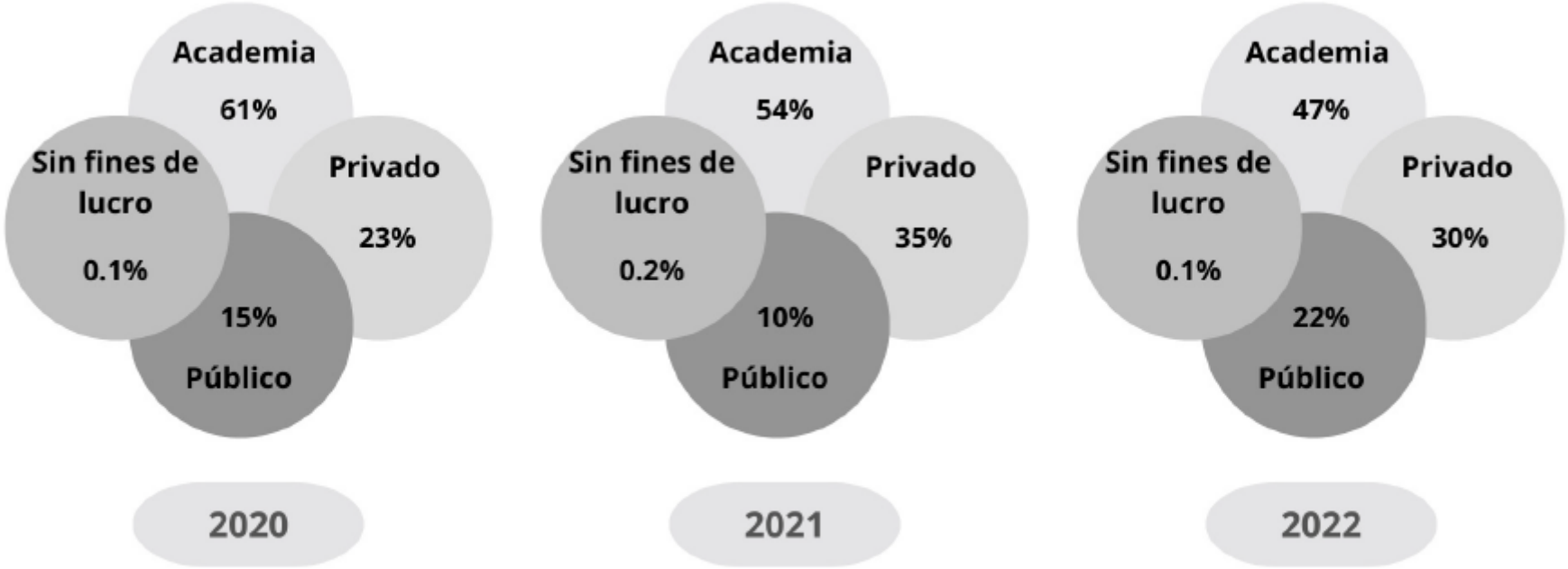
Investigación y desarrollo.

VICERRECTORÍA DE INVESTIGACIÓN
UNIVERSIDAD NACIONAL

LABORATORIO DE I + D + i
LABCIBE
EN CIBERSEGURIDAD

UNA
UNIVERSIDAD NACIONAL
COSTA RICA

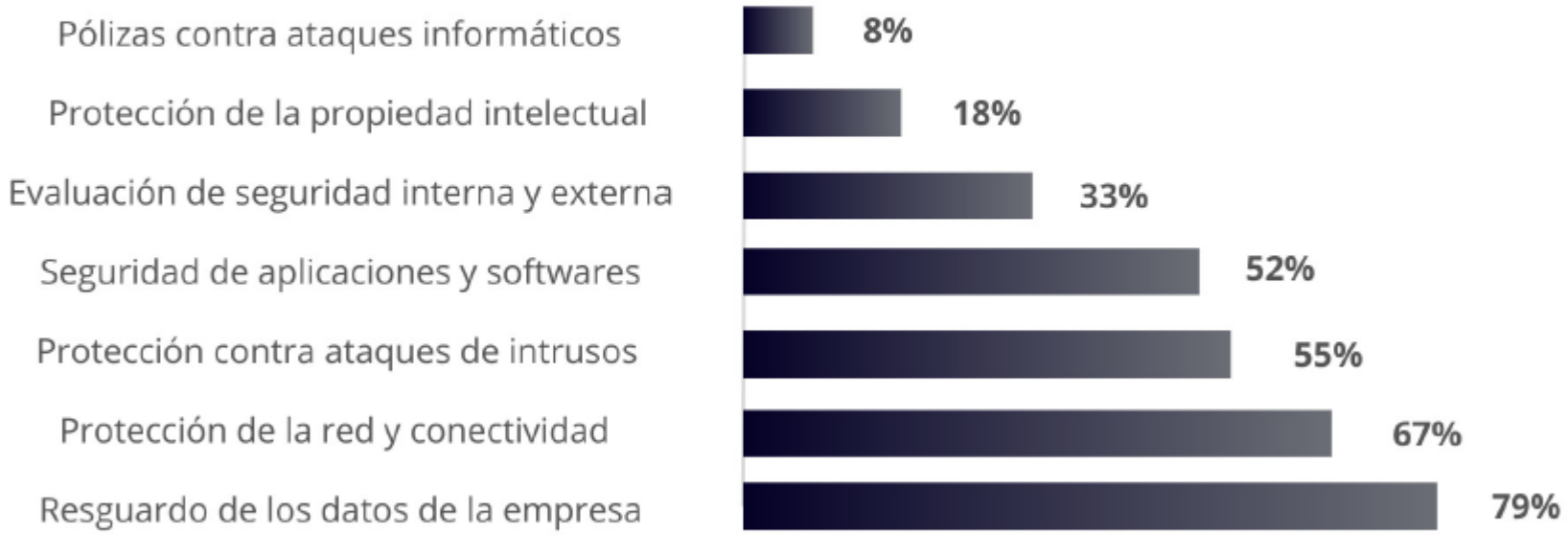
Figura 1. Distribución de Investigación y Desarrollo según sector



Fuente: Elaboración propia con base en el Informe de Indicadores Nacionales de Ciencia, Tecnología e Innovación en Costa Rica (2022).

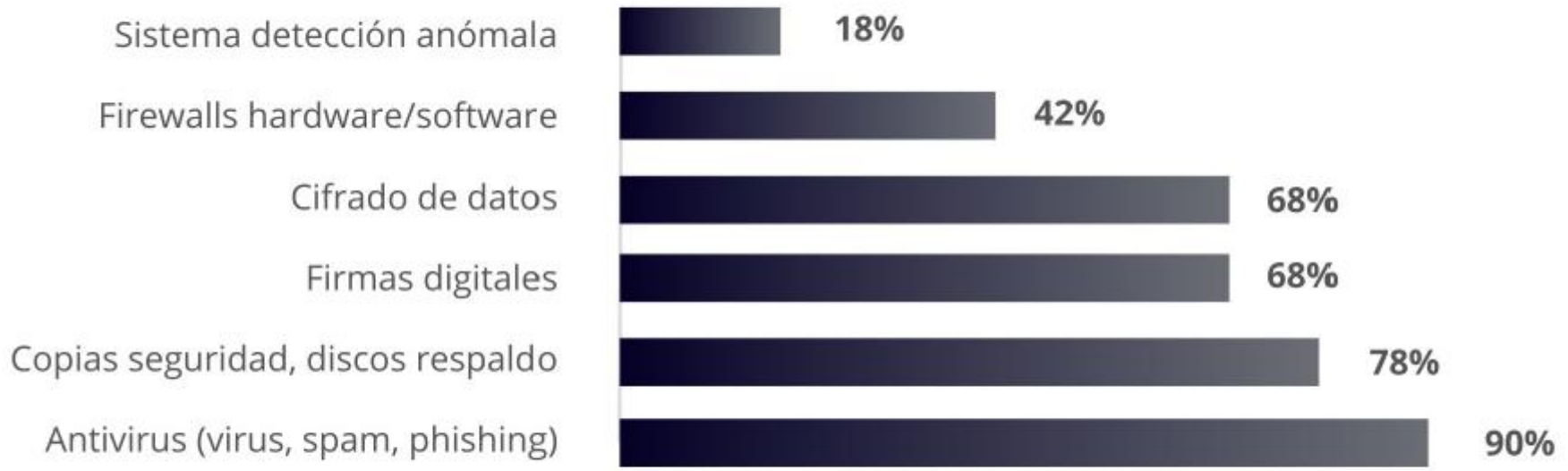
Algunos hallazgos mencionados en este estudio relacionados a la postura de ciberseguridad en las empresas son los siguientes.

Figura 2. Procesos de seguridad informática



Fuente: Elaboración propia con base en el Informe de Indicadores Nacionales de Ciencia, Tecnología e Innovación en Costa Rica (2022).

Figura 3. Mecanismos de seguridad informática



Fuente: Elaboración propia con base en el Informe de Indicadores Nacionales de Ciencia, Tecnología e Innovación en Costa Rica (2022).

Diagnóstico de la situación de la ciberseguridad en Costa Rica.

VICERRECTORÍA DE INVESTIGACIÓN
UNIVERSIDAD NACIONAL

LABORATORIO DE I + D + i
LABCIBE
EN CIBERSEGURIDAD

UNA
UNIVERSIDAD NACIONAL
COSTA RICA

Se diseñó una encuesta en línea dirigida a varios actores vinculados con la I+D+i en el ámbito de la Ciberseguridad, implicando así el sector educativo costarricense, e incluso organizaciones de distintos ámbitos en la industria; lo anterior, a fin de obtener una perspectiva más amplia y detallada sobre la dimensión regulatoria, jurídica y el de la investigación y desarrollo de la ciberseguridad a nivel nacional.

Resultados.

VICERRECTORÍA DE INVESTIGACIÓN
UNIVERSIDAD NACIONAL

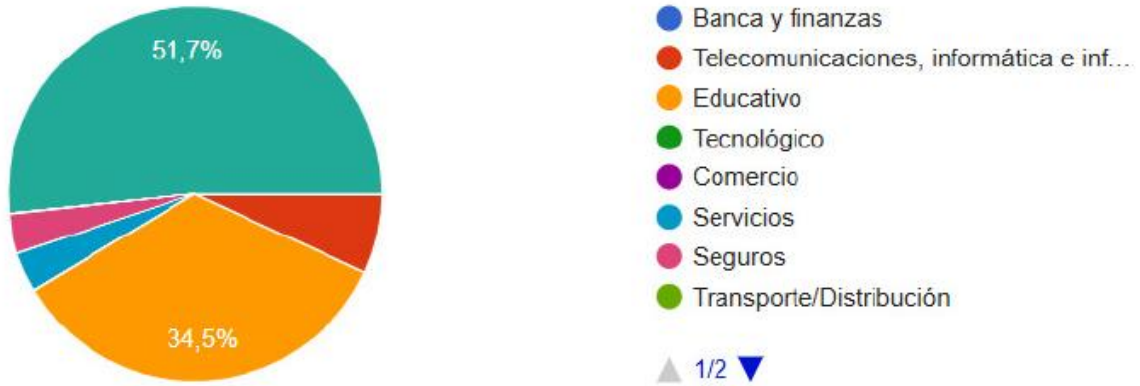
LABORATORIO DE I + D + i
LABCIBE
EN CIBERSEGURIDAD

UNA
UNIVERSIDAD NACIONAL
COSTA RICA

Participantes.

- 51,7% Sector estatal o gubernamental.
- 34,5% Sector educativo.
- 6,9% Telecomunicaciones e informática.
- 3,4% Seguros.
- 3,4% Servicios.

Gráfico 1. Distribución de resultados por sector

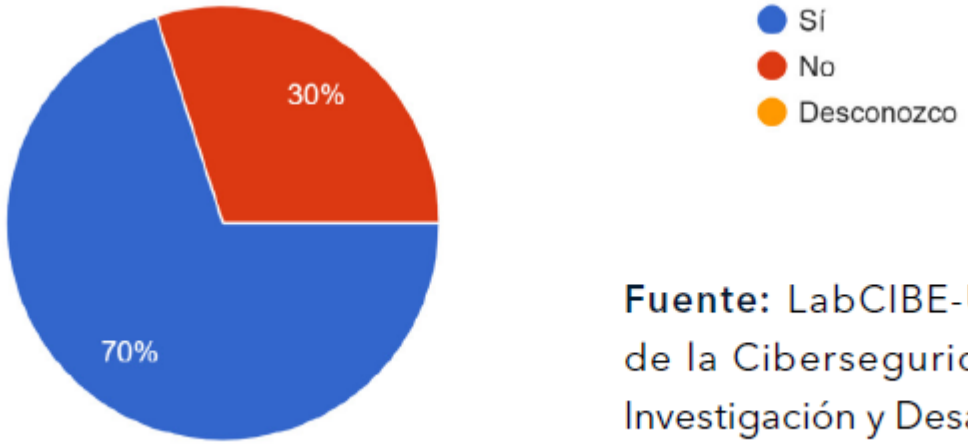


Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

Oferta de programas de formación en Ciberseguridad.

En relación a la **oferta de programas de formación** o inclusive cursos específicos en Ciberseguridad, la caída fue del 90,9% (Universidad Nacional, 2024). al 70% en el año 2024 detona que algunas instituciones percibieron poca oferta de programas de formación académica en ciberseguridad.

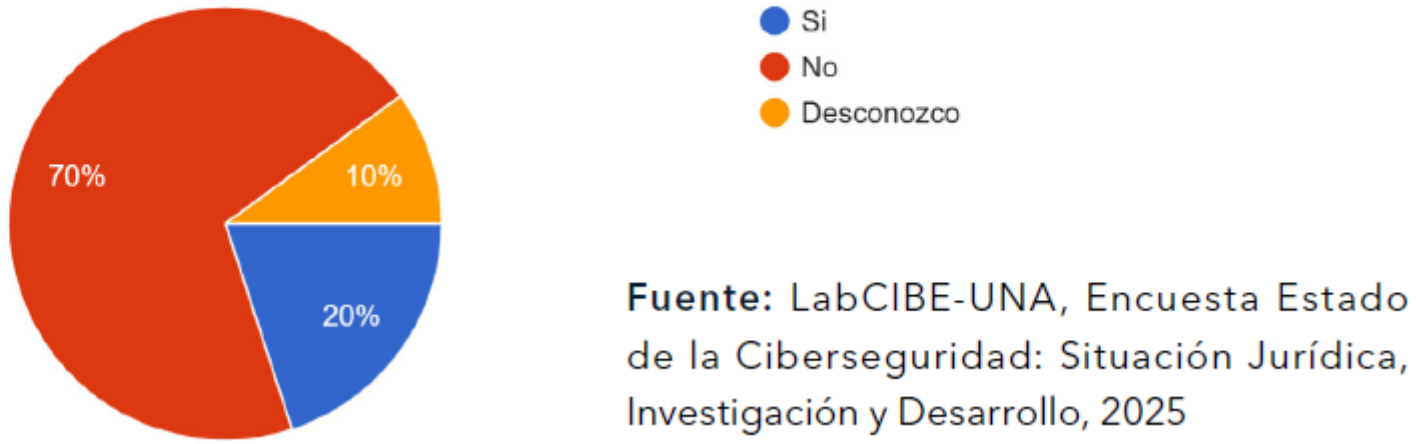
Gráfico 2. Oferta de programas de formación en ciberseguridad en instituciones educativas



Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

Presupuesto exclusivo a actividades de investigación y desarrollo en ciberseguridad.

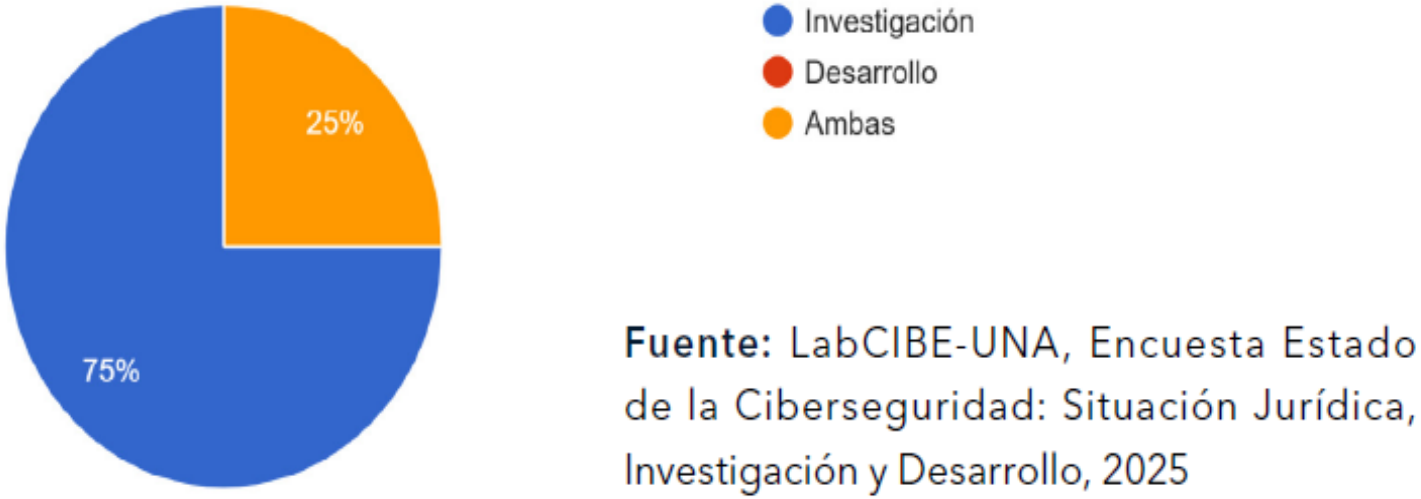
Gráfico 4. Presupuesto para I+D en ciberseguridad



Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

Investigación de Ciberseguridad.

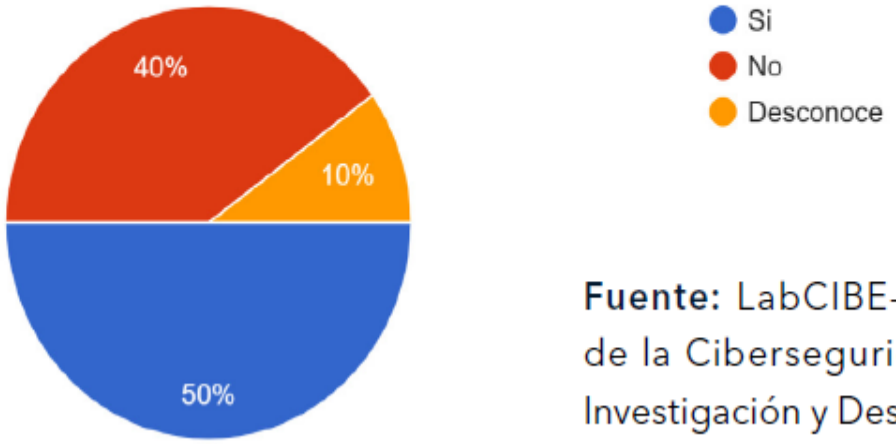
Gráfico 5. Investigación de Ciberseguridad



Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

Planes futuros para realizar proyectos de investigación y desarrollo en ciberseguridad.

Gráfico 6. Planes futuros de investigación y desarrollo en ciberseguridad



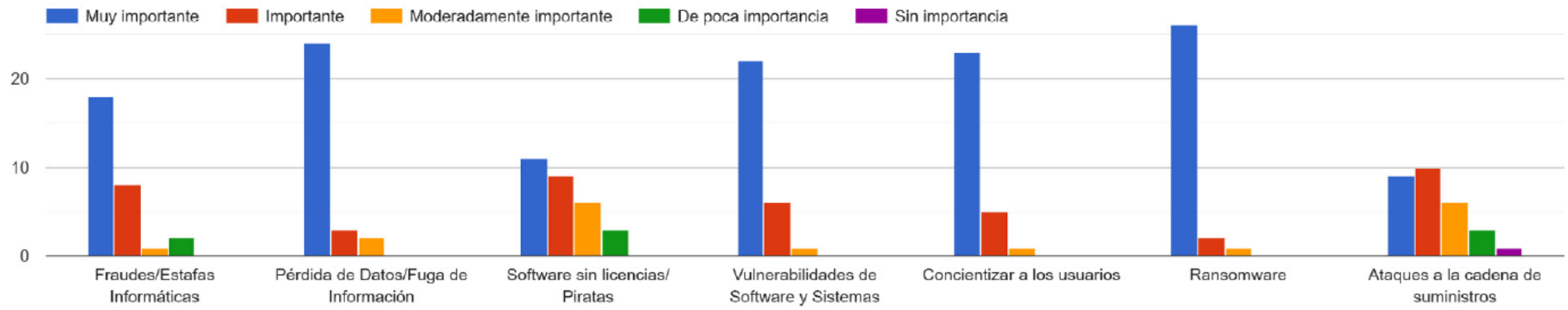
Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

Principales barreras identificadas.

- Financiamiento.
- Déficit de personal especializado.
- Limitaciones de infraestructura y datos.
- Colaboración Limitada.

Situación Jurídica de la Ciberseguridad Nacional.

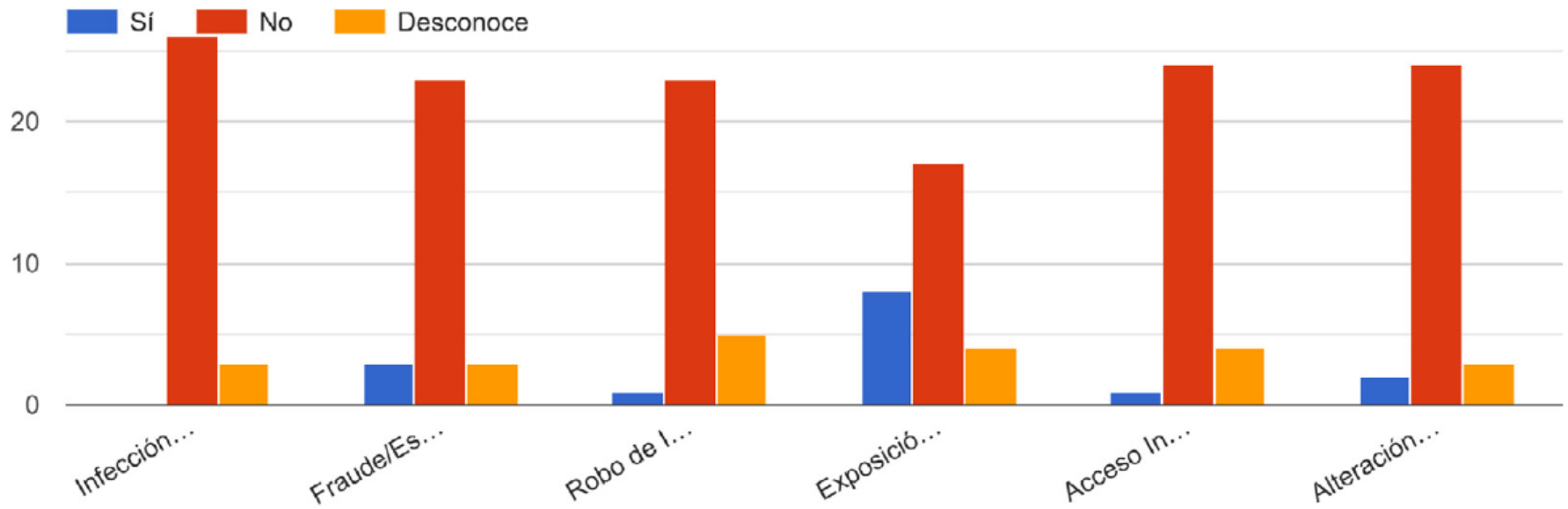
Gráfico 8. Preocupaciones en seguridad cibernética



Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

Situación Jurídica de la Ciberseguridad Nacional.

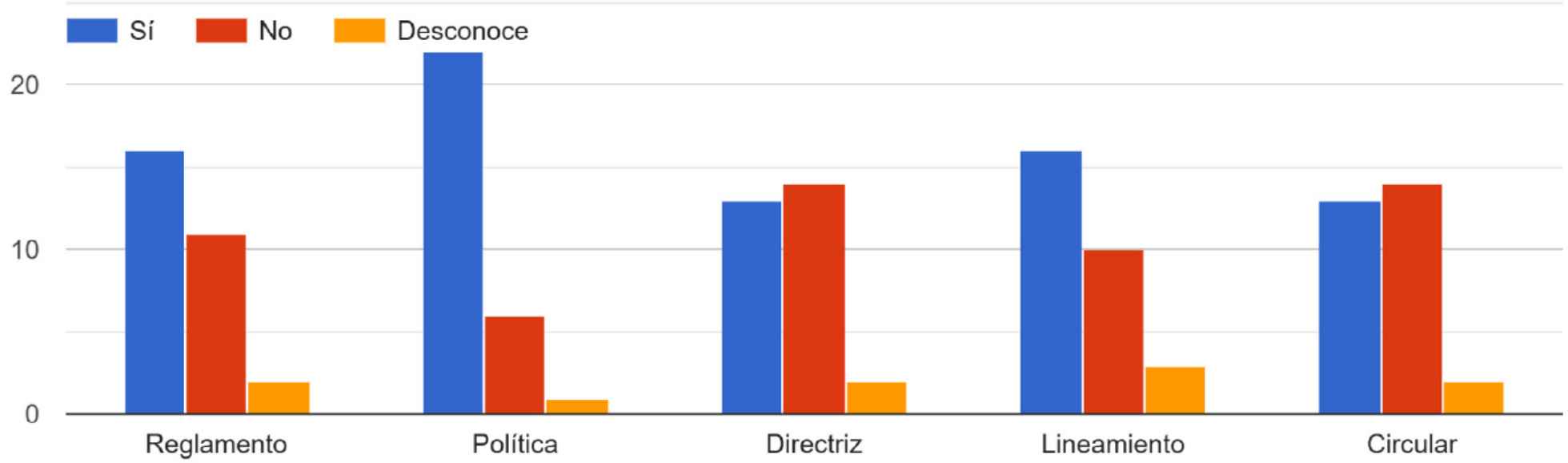
Gráfico 9 Ataques cibernéticos



Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

Estado de la Ciberseguridad.

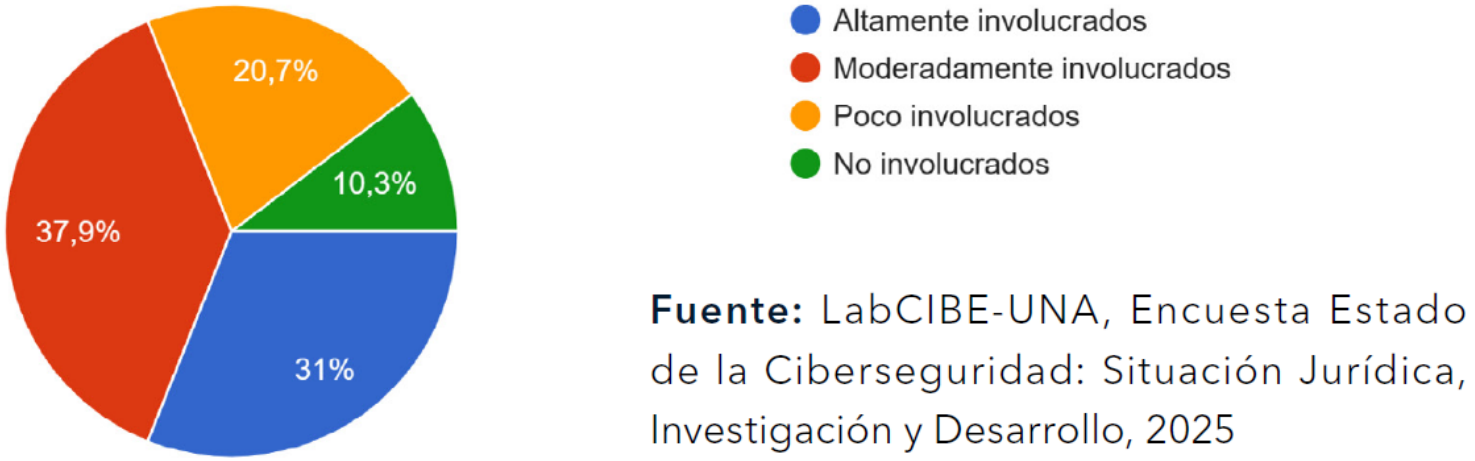
Gráfico 10. Establecimiento de normativas internas en materia de tecnologías



Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

Involucramiento de la alta dirección.

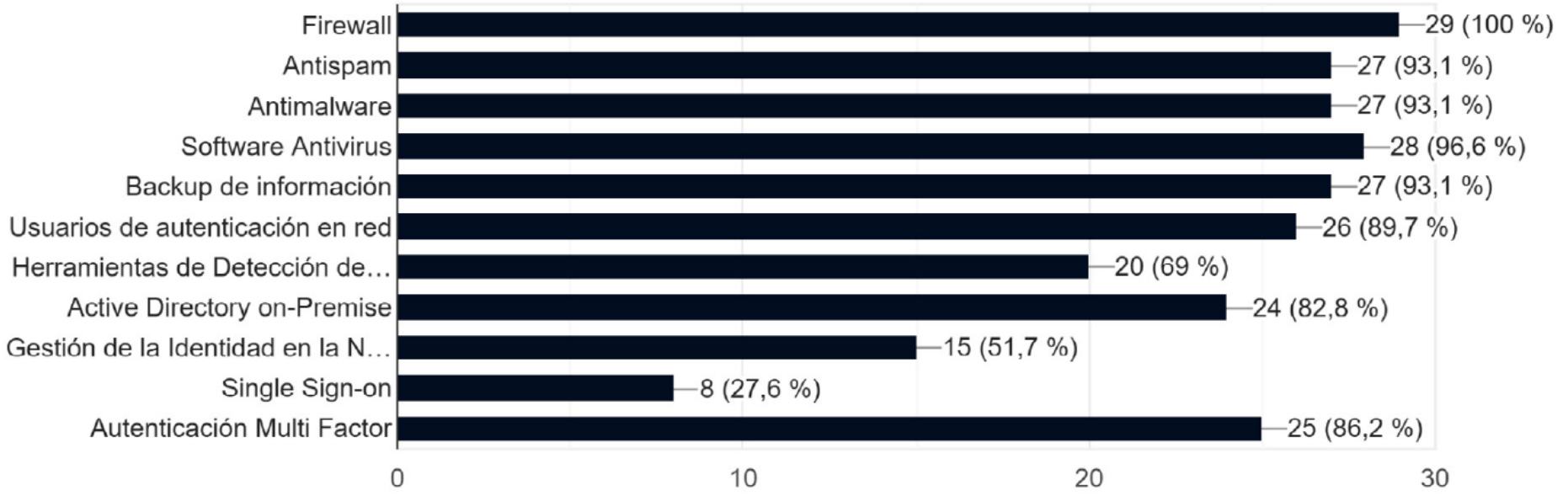
Gráfico 11. Involucramiento de la alta dirección en decisiones y políticas de ciberseguridad



Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

Principales controles de seguridad cibernética

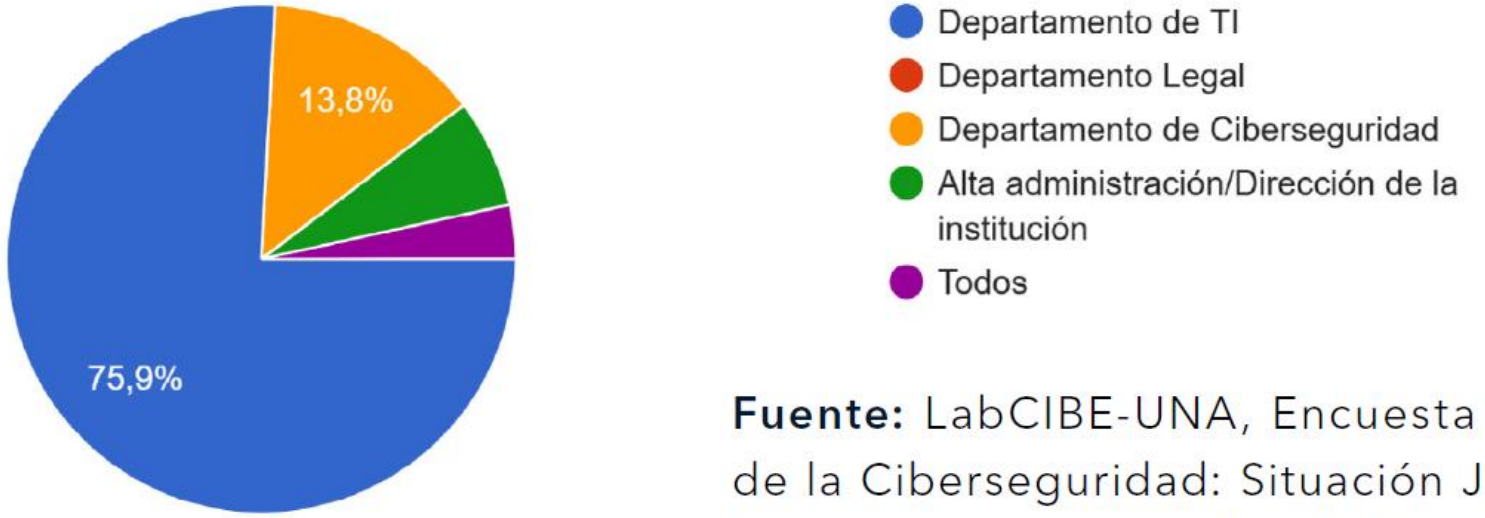
Gráfico 12. Controles de Seguridad Cibernética



Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

Prevención de incidentes.

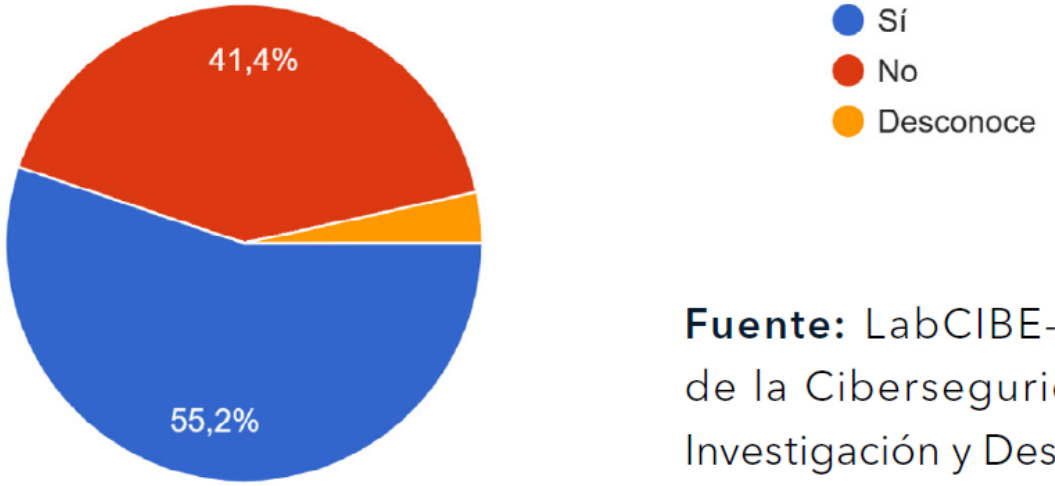
Gráfico 13. Departamentos responsables de la prevención incidente cibernéticos



Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

Prevención de incidentes.

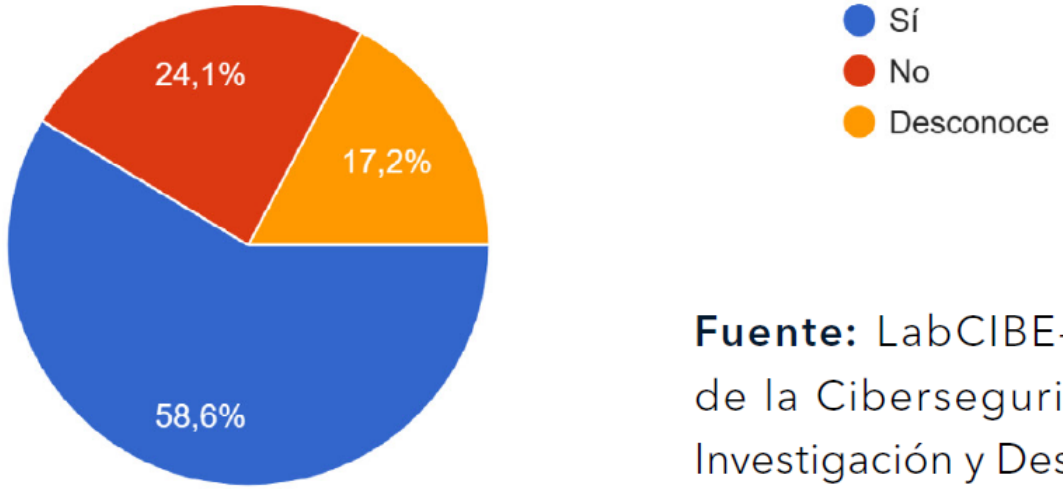
Gráfico 14. Implementación de mecanismo de evaluación de riesgo cibernético



Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

Protección de datos del cliente.

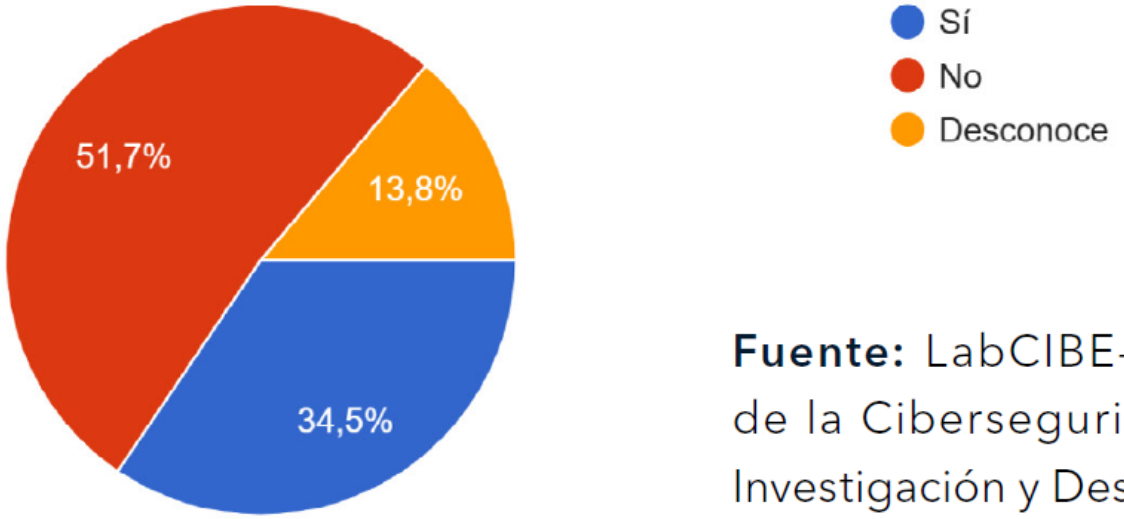
Gráfico 15. Implementación de medidas para el cumplimiento de la ley de protección de datos del cliente



Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

Frecuencia en realización de simulacros.

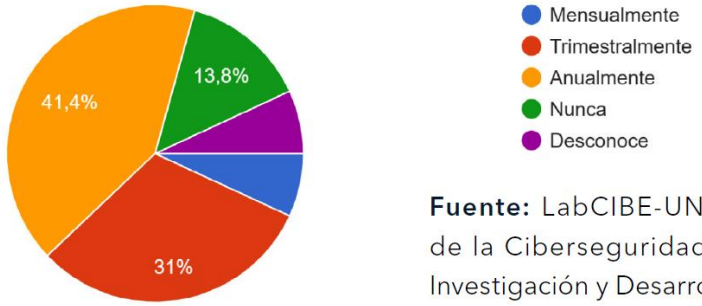
Gráfico 16. Ejecución de simulacros de seguridad



Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

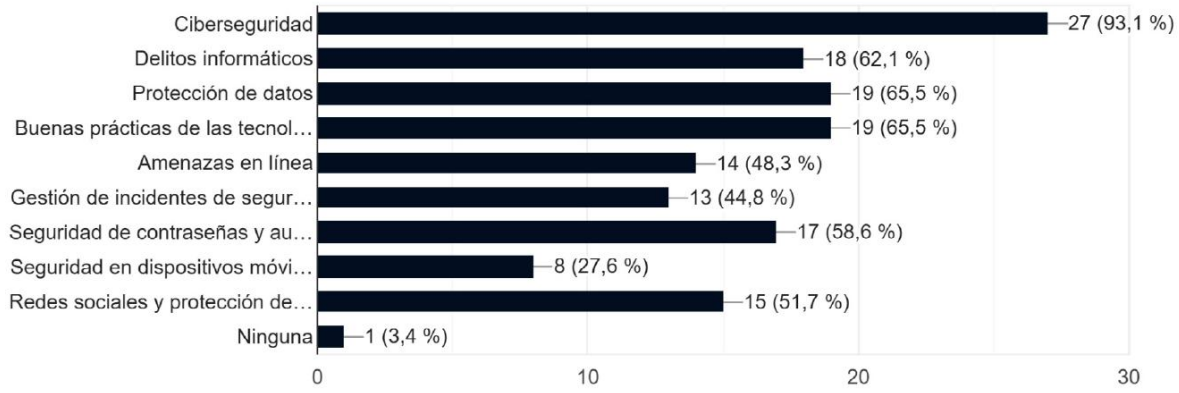
Participa u organiza conferencias y/o talleres sobre ciberseguridad.

Gráfico 17. Participación/organización de conferencias o talleres sobre ciberseguridad



Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

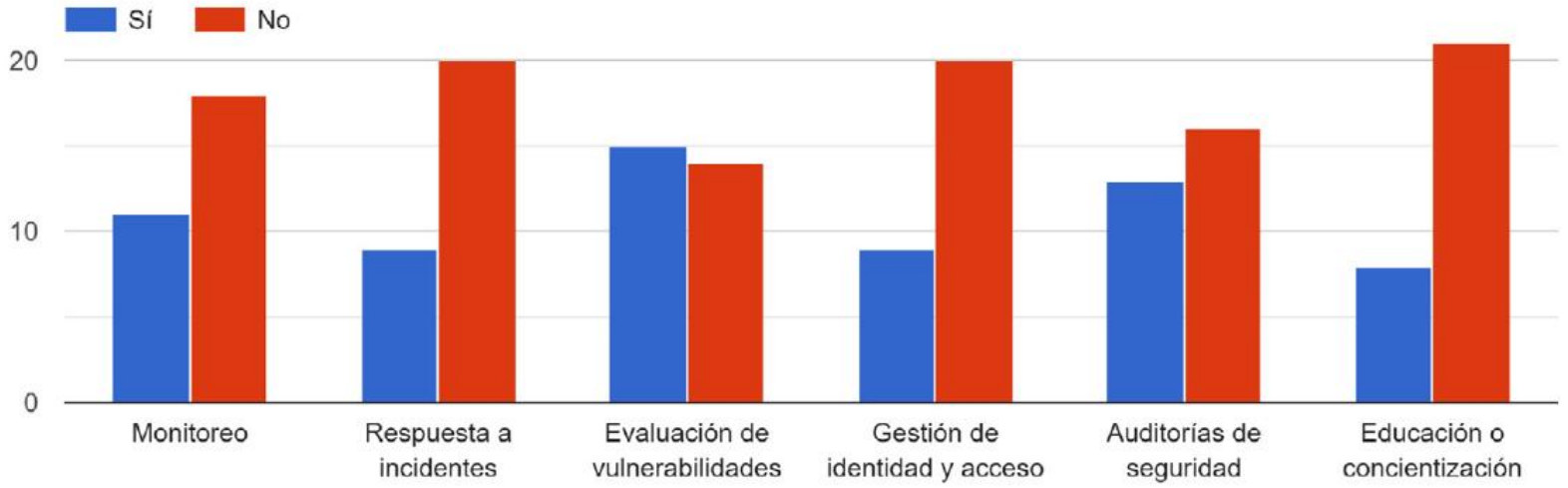
Gráfico 18. Temáticas de formación y/o capacitación



Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

Subcontratación de servicios relacionados con ciberseguridad.

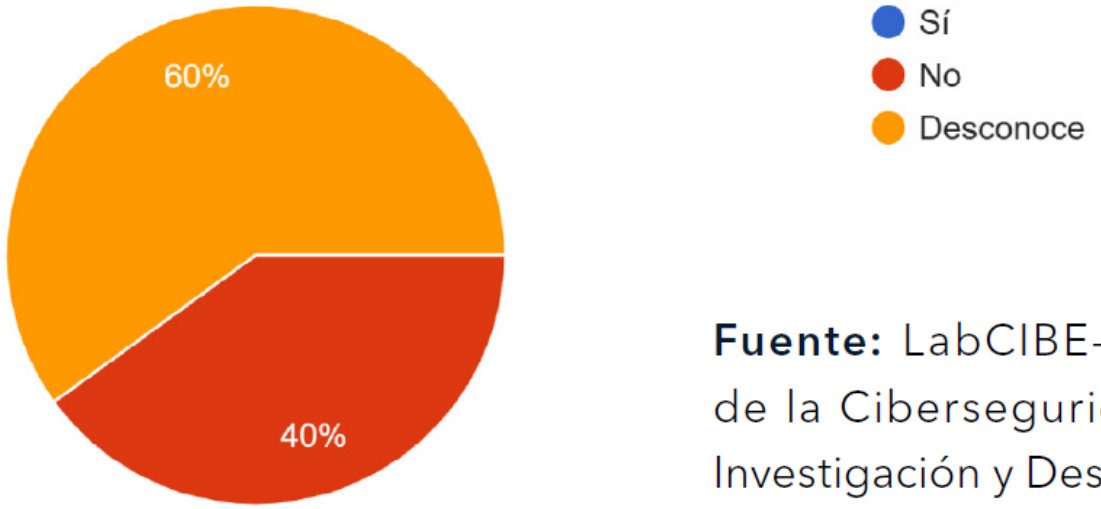
Gráfico 21. Subcontratación de Servicios



Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

Red privada para la protección de comunicaciones internas y externas.

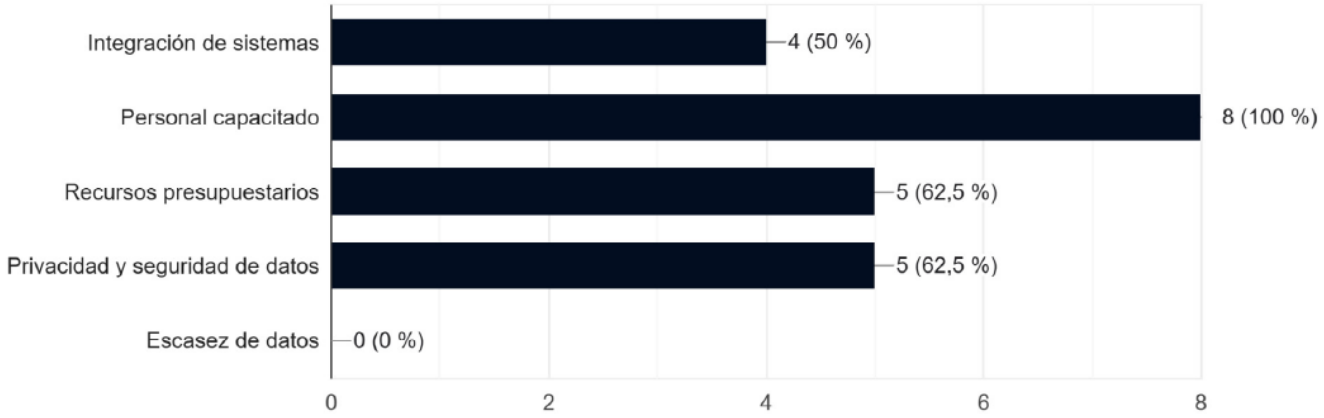
Gráfico 23. Ataques cibernéticos en mercados extranjeros



Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

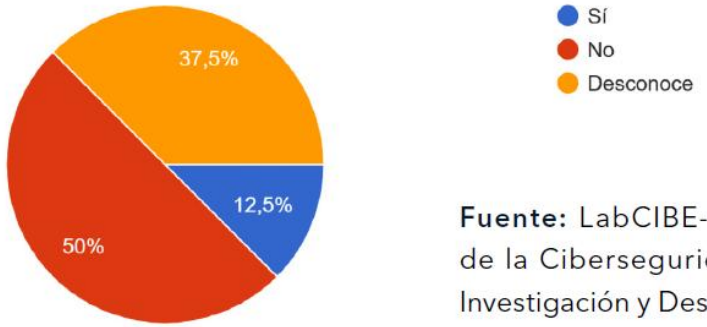
Uso de IA en la ciberseguridad.

Gráfico 24. Desafíos en la implementación de IA en ciberseguridad



Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

Gráfico 25. Personal capacitado en IA



Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

UNA UNIVERSIDAD NACIONAL COSTA RICA

Conclusiones.

VICERRECTORÍA DE INVESTIGACIÓN
UNIVERSIDAD NACIONAL

LABORATORIO DE I + D + i
LABCIBE
EN CIBERSEGURIDAD

UNA
UNIVERSIDAD NACIONAL
COSTA RICA

- Disminución de la oferta educativa especializada en ciberseguridad; para el 2023, el 90,9% de instituciones educativas ofrecían programas específicos, mientras que en el 2024, un 70%.
- Percepción de financiamiento bajo, dedicado a investigación y desarrollo en ciberseguridad.
- Percepción de la importancia en la ámbito de la ciberseguridad.
- Riesgos identificados en la organizaciones, relacionado directamente con el ransomware.
- Hay mejora en la concientización de los usuarios sobre los riesgos cibernéticos.

- Se ha logrado avanzar en temas de políticas y protocolos internos en las organizaciones, así como la implementación de procedimientos operativos.
- La formación y capacitación en ciberseguridad siendo áreas de oportunidad.
- Desafíos en el temas de IA, considerando principalmente personal capacitado en tema de IA aplicado en ciberseguridad.
- El manejo de la implementación de medida preventivas y de evaluaciones de riesgos sigue siendo unos de los principales desafíos en las organizaciones.

¡Muchas gracias!

VICERRECTORÍA DE INVESTIGACIÓN
UNIVERSIDAD NACIONAL

LABORATORIO DE I + D + i
LABCIBE
EN CIBERSEGURIDAD

UNA
UNIVERSIDAD NACIONAL
COSTA RICA

Datos importantes.

MACIBI
MAESTRÍA EN CIBERSEGURIDAD INDUSTRIAL
LABCIBE

LABORATORIO DE I + D + i
LABCIBE
EN CIBERSEGURIDAD

VICERRECTORÍA DE INVESTIGACIÓN
UNIVERSIDAD NACIONAL

LABORATORIO DE I + D + i
LABCIBE
EN CIBERSEGURIDAD

UNA
UNIVERSIDAD NACIONAL
COSTA RICA

LABORATORIO DE I + D + i
LABCIBE
EN CIBERSEGURIDAD

50 AÑOS CONARE
CONSEJO NACIONAL DE RECTORES

UNA UNIVERSIDAD NACIONAL COSTA RICA
SEDE REGIONAL CHOROTEGA

Hallazgos del informe “Estado de la Ciberseguridad en Costa Rica 2024, desde el enfoque Jurídico, Investigación y Desarrollo" LabCIBE UNA 2025.

Ing. Raymond A. Pérez Meza. M.Sc.

Académico Investigador LabCIBE.