ESTADO DE LA CIBERSEGURIDAD EN COSTA RICA 2025

WWW.UNA.AC.CR

UNA UNIVERSIDAD NACIONAL COSTA RICA

LABORATORIO DE I+D+i LABCIBE EN CIBERSEGURIDAD

VICERRECTORÍA DE INVESTIGACIÓN UNIVERSIDAD NACIONAL

005.8 Vega Briceño, Edgar.
V422e *Estado de la ciberseguridad en Costa Rica 2025* / Edgar Vega Briceño, Roberto Lemaitre Picado, Alex Villegas Carranza, Laura Flores Barrantes.
Universidad Nacional, Sede Regional Chorotega, 2026.
1 recurso en línea (166 páginas) : archivo de texto, PDF.

ISBN 978-9968-526-27-2

1.SEGURIDAD (INFORMÁTICA). 2. ANÁLISIS DE LA INFORMACIÓN. 3. REDES SOCIALES EN LÍNEA. 4. INTERNET 5. PROTECCIÓN DE DATOS. 6. PROPIEDAD INTELECTUAL.
I. Lemaitre Picado, Roberto, coautor. II. Villegas Carranza, Alex, coautor.
III. Flores Barrantes, Laura, coautora. IV. Título.

Vicerrectoría de Investigación
Sede Regional Chorotega
Laboratorio de Investigación, desarrollo e innovación en ciberseguridad (Labcibe)

Investigadores
Edgar Vega Briceño
Roberto Lemaitre Picado
Alex Villegas Carranza
Laura Flores Barrantes

Sede Regional Chorotega
Abril, 2026

Índice

Índice de tablas

Índice de gráficos

Preliminares

UNA UNIVERSIDAD NACIONAL COSTA RICA

LABORATORIO DE I+D+i LABCIBE EN CIBERSEGURIDAD

VICERRECTORÍA DE INVESTIGACIÓN UNIVERSIDAD NACIONAL

WWW.UNA.AC.CR

Presentación

El tercer informe *Estado de la Ciberseguridad en Costa Rica 2025* presenta los hallazgos derivados de la investigación anual sobre el estado de la ciberseguridad en el país, consolidando el esfuerzo iniciado en 2023 por el equipo académico del Laboratorio de Investigación, Desarrollo e Innovación en Ciberseguridad (LabCIBE), de la Sede Regional Chorotega y la Vicerrectoría de Investigación de la Universidad Nacional (UNA). Esta edición profundiza en tres ejes fundamentales: la situación jurídica y normativa, la investigación y desarrollo (I+D), y el diagnóstico situacional mediante una encuesta ampliada que contó con la participación de 143 instituciones.

El panorama de la ciberseguridad en Costa Rica continúa evolucionando de manera acelerada. Los datos oficiales del Organismo de Investigación Judicial revelan que entre 2018 y agosto de 2025 se han registrado más de 40.000 denuncias por delitos informáticos, con un crecimiento exponencial que evidencia la consolidación de la cibercriminalidad como un problema estructural de seguridad pública, económica y social. Este contexto refuerza la necesidad de contar con diagnósticos rigurosos y actualizados que orienten la toma de decisiones tanto en el sector público como en el privado.

El informe 2025 mantiene su estructura integral, iniciando con un análisis exhaustivo del marco jurídico nacional que incluye leyes, decretos, reglamentos y estrategias vigentes en materia de ciberseguridad. Posteriormente, examina el ecosistema de investigación y desarrollo, abarcando la oferta académica tanto pública como privada, las iniciativas de la industria nacional y los repositorios de investigación disponibles. Finalmente, el diagnóstico situacional incorpora nuevas dimensiones de análisis, incluyendo la adopción de inteligencia artificial, la asignación de recursos y presupuesto, y la madurez de los programas de capacitación y respuesta a incidentes. El objetivo central de este informe continúa siendo proporcionar una herramienta de consulta útil para la formulación de políticas públicas, la planificación estratégica institucional y la implementación de medidas efectivas de prevención y respuesta ante incidentes cibernéticos. Los resultados están dirigidos a autoridades del sector público y privado, organismos de seguridad nacional, empresas tecnológicas, académicos, investigadores y la sociedad civil organizada, con el propósito de fortalecer de manera colaborativa la postura de ciberseguridad del país.

Edgar Vega Briceño
Coordinador LabCIBE

Introducción

El ecosistema de ciberseguridad en Costa Rica atraviesa un momento crítico de transformación. Los datos oficiales del Organismo de Investigación Judicial correspondientes al período 2018-2025 revelan más de 40.000 denuncias por delitos informáticos, con un incremento del 96,7% entre 2023 y 2024 que marca un punto de inflexión en la trayectoria del cibercrimen nacional. Este crecimiento exponencial, donde el 84% de los casos se concentra en estafa informática y suplantación de identidad, evidencia que la cibercriminalidad ha dejado de ser un fenómeno coyuntural para consolidarse como un problema estructural que afecta la seguridad pública, económica y social del país.

La convergencia de tecnologías emergentes como la inteligencia artificial, el Internet de las Cosas y la computación en la nube ha expandido significativamente la superficie de ataque de las organizaciones. Los actores maliciosos han sofisticado sus técnicas, aprovechando modelos de ingeniería social cada vez más convincentes, vulnerabilidades de día cero y ataques dirigidos a la cadena de suministro. Este panorama demanda que las organizaciones adopten un enfoque integral de ciberseguridad que trascienda las soluciones tecnológicas para incorporar la gestión del factor humano, la resiliencia operativa y el cumplimiento regulatorio como pilares fundamentales de su estrategia de defensa.

Este tercer informe *Estado de la Ciberseguridad en Costa Rica 2025* consolida el esfuerzo de investigación iniciado en 2023, ampliando su alcance mediante una encuesta que contó con la participación de 143 instituciones de los sectores público y privado. El estudio evalúa la madurez organizacional en dimensiones críticas como la gestión de riesgos cibernéticos, la prevención y respuesta a incidentes, los programas de capacitación, la asignación de recursos y presupuesto, y la incorporación de tecnologías emergentes como la inteligencia artificial. Esta metodología permite realizar comparaciones interanuales de carácter descriptivo, orientadas a identificar tendencias y patrones relevantes, considerando las variaciones en la composición de la muestra entre cada edición e identificar tendencias significativas en la evolución de la postura de ciberseguridad nacional.

La estructura del informe se organiza en tres capítulos complementarios. El primero presenta un análisis exhaustivo del marco jurídico y normativo vigente, incluyendo las tendencias de cibercriminalidad, las leyes, decretos, reglamentos y estrategias nacionales que regulan la materia. El segundo capítulo examina el ecosistema de investigación y desarrollo, abarcando la oferta académica de universidades públicas y privadas, las iniciativas de la industria nacional y los repositorios de investigación disponibles. Finalmente, el tercer capítulo presenta el diagnóstico

situacional fundamentado en los datos empíricos de la encuesta 2025, ofreciendo una radiografía actualizada que permita a los tomadores de decisión orientar políticas públicas, estrategias institucionales y acciones concretas para fortalecer la resiliencia cibernética del país.

Situación jurídica de la ciberseguridad nacional

CAPÍTULO I

UNA UNIVERSIDAD NACIONAL COSTA RICA

LABORATORIO DE I+D+i LABCIBE EN CIBERSEGURIDAD

VICERRECTORÍA DE INVESTIGACIÓN UNIVERSIDAD NACIONAL

1.1. ¿Qué es la ciberseguridad?

La ciberseguridad es un componente esencial dentro del marco más amplio de la seguridad de la información. Se entiende como el conjunto de políticas, procesos, controles y prácticas destinados a proteger los activos de información digital frente a amenazas que afectan datos procesados, almacenados o transmitidos en sistemas y redes interconectadas. A diferencia de la seguridad de la información, que abarca todo tipo de soportes, la ciberseguridad se centra específicamente en el entorno digital, incluyendo infraestructura (*hardware* de red y equipos), aplicaciones (*software* y servicios) y datos que circulan en los sistemas informáticos (ISACA, 2021).

Pilares

- **Confidencialidad.** Garantiza que la información sea accesible solo para sujetos y procesos autorizados. Se sostiene, entre otros, mediante cifrado, autenticación y autorización robustas, segmentación de redes y uso de redes privadas virtuales (VPN) para canales de comunicación seguros.
- **Integridad.** Asegura que los datos permanezcan exactos, completos y no alterados sin autorización. Se preserva con firmas digitales, funciones *hash*, controles de cambios (control de versiones), segregación de funciones y registros de auditoría.
- **Disponibilidad.** Procura que la información y los servicios estén accesibles cuando se requieren. Se garantiza con redundancia, copias de respaldo, protección frente a denegación de servicio, arquitectura resiliente y mantenimiento/actualización sistemáticos.

A estos pilares suelen añadirse atributos complementarios, autenticidad, trazabilidad, no repudio y resiliencia operativa, que refuerzan la confianza y la continuidad del negocio frente a incidentes.

1.2. ¿Qué son las amenazas informáticas?

Una amenaza informática es cualquier acción, condición o evento capaz de perjudicar sistemas, redes o información. Sus formas y finalidades son diversas: desde el robo o la manipulación de datos personales hasta la indisponibilidad de servicios críticos. Ejemplos usuales incluyen:

- ***Malware* (incluye las categorías de virus, gusanos, troyanos y *ransomware*).** Programas diseñados para sustraer, cifrar, dañar o eliminar información; los virus se replican y diseminan automáticamente; el *ransomware* cifra activos y extorsiona.
- ***Phishing* (y variantes como *smishing*, *vishing*).** Técnicas de ingeniería social que engañan a la víctima para que revele credenciales o información financiera, o ejecute acciones riesgosas para su información personal o de la empresa.
- **Ataques de fuerza bruta y de credenciales.** Intentos automatizados para adivinar contraseñas o reutilizar credenciales expuestas.
- **Ataques de denegación de servicio distribuida (DDoS).** Saturación de recursos mediante tráfico malicioso coordinado, que impide el acceso normal a un servicio.
- ***Exploits* y vulnerabilidades (incluidos *0-day* (vulnerabilidad del día 0).** Aprovechamiento de fallas en *software* o *hardware* para escalar privilegios, ejecutar código o provocar fallas.
- **Intercepción o ataques de intermediario (*man-in-the-middle*).** Inserción no autorizada en una comunicación para leer, modificar o redirigir tráfico.

Las amenazas se materializan cuando encuentran vulnerabilidades explotables y convergen con exposición suficiente; el riesgo surge precisamente de esa relación (amenaza × vulnerabilidad × impacto), y la gestión de riesgo busca reducir la probabilidad y/o el impacto mediante controles preventivos, detectivos y de respuesta que las empresas e instituciones desarrollan para disminuir el riesgo.

1.3. Tendencias de la cibercriminalidad en Costa Rica (2018–2025)

Mediante los datos proporcionados por el Organismo de Investigación Judicial (OIJ) 2025 confirma que la cibercriminalidad mantiene una trayectoria ascendente y acelerada en el país. En el período 2018–2025, con corte al 31 de agosto 2025, se registran 40.457 denuncias por delitos informáticos, con picos notables en 2024 y 2025. Este comportamiento no es meramente cuantitativo: la composición delictiva se concentra en modalidades de estafa digital y suplantación de identidad, y la distribución territorial refleja patrones vinculados a concentración demográfica, bancarización y exposición digital, lo cual se analiza en las siguientes tablas con base en el informe oficial brindado por el OIJ, Unidad de Análisis Criminal, sobre «Delitos informáticos». El estudio brindado refleja las últimas cifras de 2025 al 31 de agosto 2025.

1.3.1. Volumen y dinámica temporal

Entre 2018 y 2025 las denuncias pasaron de 1.647 a 10.598 casos anuales, con una acumulación de 40.457 en todo el período. El punto de inflexión es 2024, que casi duplica a 2023 (10.398 vs. 5.287; +96,7 %). A agosto de 2025, el volumen ya supera el total de 2024 (+1,9 %), indicando persistencia del fenómeno. Desde 2018 a 2025, el volumen se multiplica por 6,4, lo que sugiere que la cibercriminalidad no solo crece, sino que se consolida como problema estructural de seguridad pública y económica.

Tabla 1. Denuncias por delitos informáticos por año (01/01/2018–31/08/2025)

Año	Totales
2018	1647
2019	2100
2020	2387
2021	2882
2022	5158
2023	5287
2024	10 398
2025	10 598
Total:	40 457

Fuente: OIJ, Unidad de Análisis Criminal, respuesta a solicitud 2504-OPO/UAC/S-2025, «Delitos informáticos», 01/01/2018–31/08/2025.

1.3.2. Composición delictiva

De la información suministrada el 84 % de los casos se concentra en dos categorías: estafa informática (62,1 %) y suplantación de identidad (21,7 %). En segundo plano aparecen: «otro/indeterminado», difusión de información falsa, suplantación de páginas electrónicas, espionaje informático, facilitación del delito informático, seducción/encuentro con menores por medios electrónicos, instalación/propagación de programas maliciosos, sabotaje y daño informático.

Tabla 2. Distribución por tipo de delito (2018–2025)

Delito	Casos	Porcentaje
Estafa informática	25 100	62.1 %
Suplantación de identidad	8757	21.7 %
Otro/indeterminado	2222	5.5 %
Difusión de información falsa	960	2.4 %
Suplantación de páginas electrónicas	929	2.3 %
Espionaje informático	745	1.8 %
Facilitación del delito informático	656	1.6 %
Seducción/encuentro con menores por medios electrónicos	491	1.2 %
Instalación/propagación de programas maliciosos	348	0.9 %
Sabotaje informático	151	0.4 %
Daño informático	96	0.2 %
Total:	40 457	100 %

Fuente: OIJ, Unidad de Análisis Criminal, respuesta a solicitud 2504-OPO/UAC/S-2025, «Delitos informáticos», 01/01/2018–31/08/2025.

1.3.3. Distribución territorial

Por provincias, la concentración se ubica en la GAM: San José 38 %, seguida de Alajuela 19 %, Heredia 11 % y Cartago 10 %. Guanacaste y Puntarenas rondan 7 % cada una, y Limón cerca de 5–6 %.

Tabla 3. Denuncias por provincia (2018–2025)

Provincia	Casos	Porcentaje
San José	15 447	38.2 %
Alajuela	7777	19.2 %
Heredia	4602	11.4 %
Cartago	4199	10.4 %
Guanacaste	2963	7.3 %
Puntarenas	2879	7.1 %
Limón	2219	5.5 %
Sin provincia	371	0.9 %
Total:	40 457	100 %

Fuente: OIJ, Unidad de Análisis Criminal, respuesta a solicitud 2504-OPO/UAC/S-2025, «Delitos informáticos», 01/01/2018–31/08/2025.

1.3.4. Perfil de víctimas

La serie de datos consigna 41.836 víctimas. Por sexo, mujeres 50 %, hombres 46 % y «desconocido» 4 %. Por edad, la afectación se concentra en 18–64 (86 %), con pico en 30–39 y 40–49; 65+ representa cerca del 9 %, y 12–17 el 2–3 %.

Tabla 4. Víctimas por sexo (2018–2025)

Sexo	Víctimas	Porcentaje
Mujer	20 859	49.9 %
Hombre	19 104	45.7 %
Desconocido	1873	4.5 %
Total:	41 836	100 %

Fuente: OIJ, Unidad de Análisis Criminal, respuesta a solicitud 2504-OPO/UAC/S-2025, «Delitos informáticos», 01/01/2018–31/08/2025.

Tabla 5. Víctimas por rango de edad (2018–2025)

Rango de edad	Casos	Porcentaje
0-11	170	0.4 %
12-17	1025	2.5 %
18-29	8669	20.7 %
30-39	10 524	25.2 %
40-49	8398	20.1 %
50-64	8318	19.9 %
65+	3626	8.7 %
Desconocido	1106	2.6 %
Total:	41 836	100 %

Fuente: OIJ, Unidad de Análisis Criminal, respuesta a solicitud 2504-OPO/UAC/S-2025, «Delitos informáticos», 01/01/2018–31/08/2025.

Con base en los datos analizados se confirma que la cibercriminalidad en Costa Rica dejó de ser un fenómeno coyuntural para convertirse en un problema estructural de seguridad pública, económica y social. El salto de casos observado a partir de 2022 y el quiebre de tendencia en 2024–2025 no responden solo a mayor denuncia, nos hace suponer que existen modelos delictivos estables y escalables que combinan ingeniería social, suplantación y explotación de debilidades operativas en pagos y canales digitales. En este contexto, la capacidad del Estado y del ecosistema financiero digital para prevenir, detectar y responder ya no puede descansar exclusivamente en campañas esporádicas o esfuerzos aislados.

La concentración del 84 % en estafa y suplantación sugiere que el principal «sistema operativo» delictivo es aprovechar el factor de vulnerabilidad humano: los atacantes optimizan guiones, marcas y contextos verosímiles para inducir decisiones perjudiciales a gran escala. Esto exige una prevención de alto alcance y baja complejidad, con mensajes claros, iterados y medibles; y, del lado de la oferta, la generalización de doble factor de autenticación (MFA por sus siglas en inglés) por defecto, controles para evitar la suplantación en dominios y páginas, y alertas transaccionales proactivas basadas en anomalías. En términos de investigación del cibercrimen, el énfasis debería situarse en vinculación de patrones, trazabilidad de pagos, y cooperación temprana con plataformas para preservar evidencia útil, con protocolos estandarizados.

Además, la territorialidad del fenómeno, con sobrerrepresentación de la GAM y porcentajes no despreciables en provincias costeras, indica que la exposición

digital, la bancarización y la actividad económica condicionan el riesgo. Sin embargo, el perfil etario de víctimas (18–64) advierte que la vulnerabilidad no es sinónimo de analfabetismo digital, sino de fatiga atencional, presión de tiempo y sesgos de confianza en entornos de trabajo y vida cotidiana. De ahí la pertinencia de intervenciones segmentadas por canal y edad, junto con simulaciones periódicas que transformen la cultura de reporte temprano.

Seguidamente, se presenta una revisión exhaustiva de la normativa vigente a nivel nacional, detallando las leyes, reglamentos, decretos, estrategias y directrices directamente relacionadas con la ciberseguridad. Esta sección tiene como objetivo proporcionar una comprensión del marco legal que rige la protección de la información, las infraestructuras críticas y la respuesta a incidentes cibernéticos en el país. Este panorama normativo es fundamental para entender el entorno de cumplimiento y los desafíos regulatorios que enfrentan las organizaciones en el panorama actual de amenazas cibernéticas.

1.4. Leyes

1. Ley de la Administración Financiera de la República y Presupuestos Públicos N.° 8131

La Ley de la Administración Financiera de la República y Presupuestos Públicos N.° 8131 (2001) establece las normativas económico-financieras para la gestión de fondos públicos. Esta ley se aplica a:

1. **Administración Central:** Incluye al Poder Ejecutivo y sus dependencias.
2. **Poderes Legislativo y Judicial:** También incluye al Tribunal Supremo de Elecciones y sus órganos auxiliares, respetando el principio de separación de poderes.
3. **Administración Descentralizada y Empresas Públicas del Estado.**
4. **Universidades Estatales, Municipalidades y Caja Costarricense de Seguro Social:** Están sujetos a los principios específicos del título II de la Ley y deben proporcionar información requerida por el Ministerio de Hacienda. Están parcialmente exceptuados de esta Ley.

La Ley también se extiende a entes públicos no estatales, sociedades con participación minoritaria del sector público y entidades privadas que manejen recursos públicos, bajo ciertas condiciones. Sin embargo, la Ley no se aplica a bancos públicos ni al Instituto Nacional de Seguros, excepto en aspectos específicos como la aprobación de presupuestos y lo estipulado en ciertos artículos y títulos de la Ley.

En relación con la ciberseguridad, se establecen dos artículos que definen responsabilidades por acciones en contra del *hardware* y del *software* dentro del ámbito de aplicación del régimen económico-financiero de los órganos y entes administradores o custodios de los fondos públicos:

> *Artículo 110. Hechos generadores de responsabilidad administrativa*
>
> *Además, de los previstos en otras leyes y reglamentaciones propias de la relación de servicio, serán hechos generadores de responsabilidad administrativa, independientemente de la responsabilidad civil o penal a que puedan dar lugar, los mencionados a continuación:*
>
> *[...]*
>
> *n) Obstaculizar el buen desempeño de los sistemas informáticos de la Administración Financiera y de Proveeduría, omitiendo el ingreso de datos o ingresando información errónea o extemporánea.*

ñ) Causar daño a los componentes materiales o físicos de los aparatos, las máquinas o los accesorios que apoyan el funcionamiento de los sistemas informáticos de la Administración Financiera y de Proveeduría.

Artículo 111. Delito informático

Cometerán delito informático, sancionado con prisión de uno a tres años, los funcionarios públicos o particulares que realicen, contra los sistemas informáticos de la Administración Financiera y de Proveeduría, alguna de las siguientes acciones:

a) Apoderarse, copiar, destruir, alterar, transferir o mantener en su poder, sin el debido permiso de la autoridad competente, información, programas o bases de datos de uso restringido.
b) Causar daño, dolosamente, a los componentes lógicos o físicos de los aparatos, las máquinas o los accesorios que apoyan el funcionamiento de los sistemas informáticos.
c) Facilitar a terceras personas el uso del código personal y la clave de acceso asignados para acceder a los sistemas.
d) Utilizar las facilidades del Sistema para beneficio propio o de terceros.
Estos artículos evidencian una preocupación significativa por la integridad, seguridad y correcto funcionamiento de los sistemas informáticos de la Administración Financiera y de Proveeduría.

2. Ley de protección de la niñez y la adolescencia frente al contenido nocivo de Internet y otros medios electrónicos N.° 8934

La Ley de protección de la niñez y la adolescencia frente al contenido nocivo de Internet y otros medios electrónicos N.° 8934 (2010) establece el marco regulatorio para establecimientos con acceso público a computadoras e Internet, enfocándose en el uso que realizan las personas menores de edad. Esta normativa incorpora definiciones fundamentales para delimitar su ámbito de aplicación. En primer lugar, define Internet y sitio web, permitiendo comprender el alcance de la regulación sobre los recursos en línea. Asimismo, establece el concepto de filtro como herramienta para controlar el acceso a contenido inapropiado, destacando su importancia en la protección de personas menores de edad.

La Ley también reconoce los foros virtuales como espacios en línea donde las personas menores de edad pueden interactuar con otros usuarios y que requieren supervisión o regulación. Por su parte, los conceptos de salario base y establecimientos resultan relevantes para aspectos administrativos y de cumplimiento, especialmente en lo que respecta a las sanciones o multas y los lugares en los que se aplica la Ley. Adicionalmente, la definición de otras formas de comunicación en red amplía el alcance de la normativa más allá de la navegación web para incluir

diversas modalidades de comunicación digital, como el correo electrónico, el chat y las videoconferencias.

En cuanto al contenido regulado, la Ley refiere a temas de pornografía, siendo este uno de los aspectos centrales al regular el acceso a Internet de las personas menores de edad en establecimientos públicos. Finalmente, el concepto de destinado a personas menores de edad resulta clave para determinar qué establecimientos están sujetos a la Ley, enfatizando que cualquier lugar accesible a personas menores de edad, independientemente de su propósito principal, está incluido.

A partir de estas definiciones, la Ley establece que la Superintendencia de Telecomunicaciones (SUTEL) es el órgano encargado de la supervisión, fiscalización, regulación y control de los requerimientos y estipulaciones establecidos en la normativa. La SUTEL tiene la competencia para resolver los procedimientos administrativos por incumplimientos y aplicar sus respectivas sanciones, así como para certificar a los establecimientos libres de pornografía y contenidos nocivos.

En su artículo 7, la Ley establece una obligación específica para los proveedores de servicios de Internet respecto a los filtros de contenido, añadiendo otra responsabilidad de fiscalización a la SUTEL:

> *Todo proveedor de servicios de acceso a Internet que ofrezca o venda estos servicios al público deberá incluir, dentro de su oferta de servicios, la opción de adquirir los filtros y demás programas especiales para bloquear el acceso a sitios con los contenidos indicados en el artículo 2 de esta Ley. La Sutel fiscalizará el cumplimiento de esta obligación. (Asamblea Legislativa de la República de Costa Rica, 2010, art. 7)*

Además, la normativa contempla la educación tecnológica en su artículo 8:

> *Artículo 8. Educación*
>
> *El Patronato Nacional de la Infancia, en coordinación con el Ministerio de Educación Pública, el Ministerio de Ambiente, Energía y Telecomunicaciones, el Ministerio de Ciencia y Tecnología y la Sutel desarrollarán campañas de educación para concienciar a los padres y madres de familia, las personas tutoras o las encargadas de las personas menores de edad, sobre la importancia de velar por la información a la que acceden estos, vía Internet o por algún otro medio electrónico de comunicación. (Asamblea Legislativa de la República de Costa Rica, 2010, art. 8)*

Cabe reiterar lo señalado en análisis anteriores respecto a que, dado el rápido avance tecnológico, esta ley debería revisarse integralmente para asegurar que mantiene su relevancia y efectividad en un entorno digital en constante cambio, ya

que fue concebida bajo el modelo de los cibercafés, establecimientos que antes eran comunes y que ofrecían el servicio de computadoras con conexión a Internet para navegación de usuarios mediante pago.

3. Ley General de Telecomunicaciones N.º 8642

La Ley General de Telecomunicaciones N.º 8642 (2008) regula el ecosistema costarricense de redes y servicios de telecomunicaciones desde la perspectiva de la apertura, la competencia y el resguardo de derechos. Esta normativa no se limita al tema de permisos o gestión para habilitar el negocio de telecomunicaciones, sino que establece como objeto regulatorio el uso y explotación de redes, así como la prestación de servicios en el sector de telecomunicaciones. La Ley somete a su marco a cualquier persona u organización que opere redes o brinde servicios que se originen, terminen o transiten por Costa Rica. Además, se declara de orden público y de aplicación obligatoria, lo que eleva su cumplimiento por encima de prácticas contractuales.

En el contexto de ciberseguridad y seguridad de la información, esta ley resulta pertinente para el análisis, ya que entre sus objetivos se encuentra proteger derechos mediante garantías de continuidad, calidad, cobertura e información, así como asegurar la privacidad y confidencialidad de las comunicaciones. Estos principios se convierten en normas vinculantes a través de la inviolabilidad del tráfico y la protección de datos personales que recaen sobre operadores y proveedores, quienes deben implementar medidas técnicas y administrativas adecuadas para su cumplimiento.

En cuanto a la arquitectura institucional, la SUTEL constituye el eje operativo como órgano de la ARESEP encargado de regular, supervisar y controlar el ordenamiento jurídico del sector. De igual forma, la Ley faculta a la SUTEL para velar por el cumplimiento de las disposiciones de protección al usuario y, en el ámbito del mercado, para conducir y aplicar el régimen de competencia.

4. Ley de Certificados, Firmas Digitales y Documentos Electrónicos N.º 8454

La Ley de Certificados, Firmas Digitales y Documentos Electrónicos N.º 8454 (2005) establece el marco de validez jurídica de los documentos y firmas en soporte electrónico en Costa Rica. Su punto de partida es amplio, ya que en el artículo 1 establece que aplica a «toda clase de transacciones y actos jurídicos, públicos o privados», salvo que exista disposición legal en contrario o que la naturaleza o formalidades del acto concreto sean incompatibles con el medio electrónico. Además, faculta expresamente al Estado y a todas las entidades públicas para utilizar certificados, firmas digitales y documentos electrónicos dentro de su competencia, lo

que brinda la ruta para el tránsito hacia expedientes, trámites y actuaciones digitales de la Administración Pública mediante firma digital certificada.

El eje técnico-jurídico de esta normativa, propiamente en firma digital certificada, es el principio de equivalencia funcional: cualquier manifestación representativa o declarativa emitida por medios electrónicos es jurídicamente equivalente a su soporte físico, sin que ello dispense de los requisitos y formalidades que otras leyes exijan para actos específicos. De esta forma, la digitalización no elimina formalidades (por ejemplo, solemnidades registrales o notariales), sino que traslada la equivalencia al soporte y a la forma de acreditación.

A efectos probatorios, la Ley establece con claridad que los documentos electrónicos con firma digital certificada se califican como públicos o privados y tienen la misma fuerza probatoria que sus equivalentes en papel. Si se encuentran firmados de manera adecuada con firma digital certificada, el artículo 10 introduce una presunción de autoría y responsabilidad a favor del titular del certificado vigente, salvo prueba en contrario. En el ámbito público, el estándar es aún más exigente, puesto que los documentos públicos electrónicos deben llevar firma digital certificada. En ambos escenarios, se establece que existe una clara trazabilidad de autoría y la integridad de los documentos. Resulta importante considerar el artículo 5, que establece los usos válidos y excepciones. Tras la reforma introducida por la Ley N.º 10181 (2024), el listado de actos que no pueden consignarse en formato electrónico quedó actualizado. Se excluyen, entre otros, las disposiciones por causa de muerte salvo supuestos específicos, los actos personalísimos y los actos de familia no jurisdiccionales. Esta actualización refuerza la coherencia del sistema con otras leyes, lo que hace importante que, para el diseño de procesos digitales, sea necesario mapear formalidades antes de automatizar: no todo puede migrarse a soporte electrónico, y la Ley ahora lo establece con mayor claridad.

Junto a la Ley, el Reglamento a la Ley N.º 8454 (Decreto Ejecutivo N.º 33018-MICIT, 2006) operativiza los requisitos y remite a estándares técnicos. Destaca la referencia a la Norma INTE/ISO 21188, sobre gestión de infraestructura de clave pública para servicios financieros, como base para el contenido, emisión, suspensión, revocación y expiración de certificados. De igual forma, el Reglamento habilita a la Dirección de Certificadores de Firma Digital (DCFD) para dictar políticas específicas en la materia.

5. Ley de Creación de la Agencia Nacional de Gobierno Digital N.º 9943

La Ley de Creación de la Agencia Nacional de Gobierno Digital N.º 9943 (2020) crea la Agencia Nacional de Gobierno Digital (ANGD) como órgano ejecutor del Estado para llevar a la práctica los proyectos y servicios transversales de gobierno digital.

La ANGD opera bajo la rectoría del MICITT, con independencia operativa, y tiene el objetivo de implementar y operar servicios y proyectos digitales comunes para que la ciudadanía acceda a trámites y servicios de manera simple, ágil, segura y transparente en toda la Administración Pública.

En este contexto, la Ley reconoce el derecho de las personas a relacionarse digitalmente con el Estado y establece un mandato operativo para que las instituciones inicien planes de trabajo orientados a incorporar tecnologías de información. Estos planes deben asegurar la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad, la ciberseguridad y la conservación de datos, con referencia expresa a la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales N.° 8968 (2011). De esta manera, la Ley busca trasladar la digitalización de la categoría de «proyecto» a la de obligación de servicio, con parámetros de seguridad de carácter obligatorio.

Por otra parte, la normativa establece un marco de definiciones comunes como gobierno digital, transformación digital e interoperabilidad. Los servicios comunes que opera la ANGD son de uso obligatorio para que las instituciones brinden sus servicios, y deben estar alineados con la política pública del ente rector y publicados en un catálogo accesible.

En términos operativos, esto significa estandarización técnica y semántica, reducción de duplicidades y una base común de identidad digital, intercambio de información y plataformas compartidas. La ANGD actúa como ejecutora técnica de la interoperabilidad y es responsable de emitir guías para su adopción. Esta estructura traslada el desarrollo de los temas digitales del plano declarativo al operativo, con una agencia que ejecuta y una rectoría que define la política pública. Este modelo permite una alineación efectiva con los principios de protección de datos y seguridad digital, elementos fundamentales para sostener la confianza y la seguridad jurídica del ecosistema digital costarricense.

6. Ley para Regular el Teletrabajo N.° 9738

La Ley para Regular el Teletrabajo N.° 9738 (2019) convierte el teletrabajo en una modalidad formal de empleo para todo el sector privado y la Administración Pública, central y descentralizada, incluido el régimen municipal. Su objetivo es promover el empleo y modernizar las organizaciones mediante el uso de tecnologías de información y comunicación (TIC).

La Ley establece que el teletrabajo es voluntario y se rige por el acuerdo entre las partes, en respeto del Código de Trabajo y de los instrumentos de derechos humanos y laborales aplicables. Puede pactarse desde el inicio de la relación laboral o con

posterioridad. Cuando se acuerda después del inicio de la relación, la revocatoria debe seguir un procedimiento, estar justificada y notificarse con al menos diez días naturales de anticipación. En todo caso, la Ley reafirma que es la persona empleadora quien puede otorgar y revocar la modalidad bajo estas condiciones.

En cuanto a las responsabilidades de la persona empleadora, la Ley exige proveer y mantener equipos, programas y energía eléctrica, o documentar la excepción cuando la persona teletrabajadora voluntariamente usa equipo propio. Asimismo, debe capacitar en su uso, informar sobre riesgos, velar por la salud ocupacional, coordinar la continuidad ante interrupciones y reconocer el salario cuando la persona teletrabajadora no pueda laborar por causas imputables a herramientas o sistemas de la organización que hayan sido debidamente reportadas.

Cuando se utiliza equipo personal, debe asegurarse el acceso de la persona empleadora a la información de carácter laboral, respetando la intimidad y dignidad de la persona trabajadora. El deber de confidencialidad se relaciona estrechamente con la gestión de seguridad de la información y ciberseguridad de cualquier organización.

Para la persona teletrabajadora, además de cumplir con metas y políticas establecidas, la Ley reconoce el derecho a la desconexión digital fuera de la jornada laboral, salvo en casos de urgencia, reforzando el equilibrio entre trabajo y descanso.

7. Reforma al Código Penal - Ley N.º 9048

La reforma penal costarricense en materia de delitos informáticos se materializó mediante dos instrumentos legislativos consecutivos. La Ley de Fortalecimiento de la Legislación contra Fraude Informático y Delitos Informáticos N.º 9048 (2012) incorporó un catálogo específico de delitos informáticos y conexos, ajustando tipos penales tradicionales para hacerlos operativos en entornos digitales. Posteriormente, la Ley N.º 9135 (2013) introdujo correcciones a los delitos recién creados y afinó la tutela de la privacidad de las comunicaciones y la protección de datos personales.

Con estas reformas, el país pasó de un vacío normativo a un marco penal coherente que permite investigar y sancionar conductas como acceso y manipulación de sistemas, propagación de *malware* (programas informáticos maliciosos), suplantación de identidad, suplantación de sitios web, daño y sabotaje de información. Se establecieron, Además, agravantes cuando los ataques impactan sistemas públicos o financieros. La Ley N.º 9048 reordenó la Sección VIII del Título VII del Código Penal para alojar estos tipos penales y fijó reglas de coordinación con figuras afines como extorsión, espionaje y difusión de información falsa que comprometa la estabilidad del sistema financiero, subsanando vacíos que antes complicaban la persecución penal.

Delitos clásicos adaptados al entorno digital

Entre los ejes de tutela clásicos adaptados al entorno digital destacan dos figuras principales. En primer lugar, la violación de correspondencia o comunicaciones, regulada en el artículo 196, sanciona apropiarse, interceptar o desviar comunicaciones sin autorización, con agravantes para personal encargado de la recolección o salvaguarda de documentos o de la administración o soporte de redes y sistemas. En segundo lugar, la violación de datos personales, establecida en el artículo 196 bis, penaliza acceder, copiar, transmitir, vender o tratar sin autorización datos almacenados en sistemas o contenedores electrónicos. Esta figura prevé agravantes cuando intervienen administradores, cuando la información es sensible o cuando la víctima es persona menor de edad o incapaz.

Delitos informáticos de naturaleza económica

El núcleo económico del cibercrimen se estructura en dos planos. Primero, la estafa informática prevista en el artículo 217 bis sanciona manipular o influir en el ingreso, procesamiento o resultado de datos en sistemas automatizados, mediante datos falsos, incompletos, programación o artificios tecnológicos, para procurarse un beneficio indebido. Las penas son superiores si el hecho recae sobre sistemas públicos, bancarios o financieros, o si lo comete personal con acceso privilegiado.

Segundo, los delitos de daño y sabotaje informático, regulados en los artículos 229 bis y 229 ter, castigan la supresión, modificación, destrucción o inutilización de información, o el entorpecimiento del funcionamiento de sistemas. Se establecen agravantes cuando el impacto es social, el sistema es público o el autor abusa de posiciones de confianza técnica. En conjunto, estas figuras protegen la integridad operativa de sistemas y la confianza en transacciones digitales.

Delitos del ecosistema digital

En el ámbito del ecosistema digital, la Sección VIII incorporó figuras relacionadas con identidad y vectores de ataque. El artículo 230 tipifica la suplantación de identidad, mientras que el artículo 231 regula el espionaje informático. Por su parte, el artículo 232 penaliza la instalación y propagación de programas maliciosos, con un elenco de hipótesis que van desde inducir al usuario a instalar el programa hasta introducir código malicioso en sitios legítimos o vender servicios de denegación de servicio.
El artículo 233 sanciona la suplantación de páginas electrónicas, conducta típica del *phishing*, con agravante si se captura información confidencial. Además, se incorpora la facilitación del delito informático en el artículo 234 y agravación por crimen organizado o narcotráfico en el artículo 235. También se prevé la difusión de información falsa por medios electrónicos cuando sea capaz de distorsionar o dañar

la estabilidad del sistema financiero, revelando una preocupación temprana por la incidencia sistémica de campañas de desinformación en mercados.

Retos de aplicación

Transcurrida más de una década desde su promulgación, los retos de aplicación no son menores. Las investigaciones dependen de capacidad forense especializada, tiempos ágiles para aseguramiento de evidencia digital y cooperación interinstitucional, incluida la coordinación con el Ministerio Público y órganos especializados. Al mismo tiempo, nuevos fenómenos como el *malware* como servicio, las *botnets* (ordenadores «zombi») y las suplantaciones a gran escala tensionan la frontera entre lo tipificado y lo emergente.

Si bien la reforma penal habilitó un lenguaje jurídico actualizado para la ciberdelincuencia y elevó las exigencias de diligencia para quienes custodian información y operan infraestructuras críticas, su eficacia práctica depende de subsanar las brechas en detección temprana, respuesta técnica y capacidad investigativa, así como de mantener coherencia con marcos normativos relacionados, como la protección de datos personales y la regulación de firmas y documentos electrónicos.

8. Ley de protección de la persona frente al tratamiento de sus datos personales N.° 8968 y Decreto Ejecutivo N.° 37554-JP - Reglamento a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales

La Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales N.° 8968 (2011) constituye el pilar fundamental del régimen costarricense de privacidad. Su objetivo es garantizar el respeto a los derechos fundamentales, en particular el derecho a la autodeterminación informativa, frente al tratamiento de datos personales, cualquiera sea el medio (manual o automatizado) y el sector (público o privado).

Ámbito de aplicación

La aplicación de la Ley alcanza toda base de datos, salvo los registros de uso exclusivamente personal, interno o doméstico que no se comercialicen. Estas bases de datos no se deben registrar en la Agencia de Protección de Datos de los Habitantes (PRODHAB), pero ello no significa que la normativa no se aplique en caso de algún uso irregular o no permitido por ley.

Principios y derechos

El bloque de principios y derechos exige informar previamente y de forma clara a la persona titular sobre la existencia y finalidad de la base de datos, los destinatarios, el carácter obligatorio o facultativo de la información, el tratamiento que se dará, las consecuencias de no suministrar los datos, las vías para ejercer derechos y la identidad del responsable. Además, se debe obtener el consentimiento expreso de la persona titular, salvo en los supuestos establecidos por la misma normativa: orden judicial, datos de acceso público o mandato constitucional o legal.

La Ley consagra el principio de calidad de la información, que exige actualidad, veracidad, exactitud y adecuación a la finalidad del tratamiento. De igual forma, incorpora una pauta de conservación que establece no mantener datos que puedan afectar al titular más allá de diez años, salvo que exista norma especial, requiriendo desasociación si se necesita conservarlos por más tiempo.

En igual línea, la Ley reconoce los derechos que tradicionalmente se les conoce como ARCO (Acceso, Rectificación, Cancelación (Supresión en nuestro caso) y Oposición), que deben tramitarse y resolverse en cinco días hábiles, de forma gratuita para la persona titular.

Autoridad de control

En términos administrativos, este enorme reto recae en la Agencia de Protección de Datos de los Habitantes (PRODHAB), órgano de desconcentración máxima adscrito al Ministerio de Justicia y Paz, con potestades de supervisión, registro, inspección, resolución de reclamos, emisión de órdenes correctivas y sanción, según lo establece el artículo 28 de la Ley.

La normativa permite y fomenta que los responsables emitan protocolos de actuación para el manejo de datos. Si estos protocolos se inscriben ante PRODHAB, generan una presunción *iuris tantum* de cumplimiento. La PRODHAB también lleva el registro de bases de datos y dicta directrices para el sector público.

Transferencias de datos

En materia de transferencias, incluidas las internacionales, la regla general es el consentimiento expreso y válido de la persona titular, respetando los principios y derechos establecidos en la Ley. El Reglamento a la Ley N.° 8968, aprobado mediante Decreto Ejecutivo N.° 37554-JP (2012, reformado por Decreto N.° 40008, 2017), precisó que no se considera transferencia el traslado de datos a un encargado o proveedor, o a empresas del mismo grupo de interés económico. De igual forma, el

Reglamento desarrolló requisitos operativos para el tratamiento y la seguridad de los datos.

Registro y cánones

La Ley obliga a inscribir en PRODHAB toda base de datos, pública o privada, administrada con fines de distribución, difusión o comercialización. No deben confundirse estas bases con las puramente internas. La normativa establece cánones económicos: un canon anual por regulación y administración de doscientos dólares estadounidenses (USD 200) y otro por comercialización de consultas que varía entre USD 0,25 y USD 1 por transacción, según lo definen y regulan el Reglamento y sus reformas.

Estas reglas operan junto con el régimen de sanciones establecido en el artículo 28, que tipifica faltas leves y graves con multas calculadas en salarios base.

Perspectivas de reforma

Al momento de esta investigación, continúan en discusión en la Asamblea Legislativa propuestas de reforma integral para modernizar la normativa vigente (expedientes legislativos N.º 22.388 y N.º 23.097). Estas iniciativas enfatizan el reforzamiento de principios, la ampliación de derechos, la obligatoriedad de notificación de brechas de seguridad y la actualización de la autoridad de control. A la fecha, no se ha publicado una nueva ley. Resulta conveniente dar seguimiento a su evolución por el impacto directo que tendrá en las bases legales del tratamiento de datos, el régimen de sanciones y los deberes de reporte.

9. Adhesión de la República de Costa Rica al Convenio de Budapest sobre Ciberdelincuencia

El Convenio sobre Ciberdelincuencia del Consejo de Europa, conocido como Convenio de Budapest, fue adoptado el 23 de noviembre de 2001 y entró en vigor el 1 de julio de 2004. Este instrumento internacional representa el único tratado multilateral vinculante que abarca de manera integral todas las áreas relevantes de la legislación sobre ciberdelincuencia, incluyendo derecho penal sustantivo, derecho procesal penal y cooperación internacional.

Costa Rica ratificó el Convenio mediante la Ley N.º 9452 (2017), promoviendo una política penal común contra la ciberdelincuencia y fomentando la cooperación internacional para generar una efectiva persecución judicial de estos delitos. Es importante destacar que el país estableció tres declaraciones interpretativas al momento de la ratificación, publicadas en La Gaceta, Alcance N.º 202 de 18 de agosto de 2017, mediante el Decreto Ejecutivo N.º 40546-RREE (2017). Estas declaraciones

se relacionan con delitos contra la propiedad intelectual, la extradición de personas costarricenses por delitos informáticos y la designación de un punto de contacto para asistencia en investigaciones de ciberdelincuencia, función asignada al Poder Judicial.

Relevancia del Convenio en el contexto de la ciberdelincuencia

La relevancia del Convenio de Budapest en el contexto de la ciberdelincuencia se puede analizar desde varios aspectos fundamentales. En primer lugar, el Convenio proporciona un marco legal coherente y armonizado para la persecución de delitos cibernéticos. Al establecer un conjunto común de definiciones y tipos penales, facilita la cooperación internacional en la investigación y procesamiento de estos delitos, que por su naturaleza trascienden las fronteras nacionales.

En segundo lugar, el instrumento define y tipifica una gama amplia de conductas delictivas en el espacio digital, incluyendo el acceso ilegal a sistemas informáticos, la interferencia de datos y sistemas, el fraude informático, la pornografía infantil y otros delitos relacionados con la explotación de tecnologías de información. Esta tipificación asegura que todos los países firmantes cuenten con un estándar mínimo común de delitos penales en sus legislaciones nacionales.

Finalmente, el Convenio fomenta la colaboración entre los Estados parte, facilitando la asistencia legal mutua y el intercambio de información. Esta cooperación resulta esencial dado que la naturaleza de la ciberdelincuencia frecuentemente implica actores, infraestructuras y recursos distribuidos globalmente, lo que requiere mecanismos ágiles de coordinación transnacional para una respuesta efectiva.

10. Segundo Protocolo Adicional al Convenio sobre la Ciberdelincuencia, Relativo a la Cooperación Reforzada y la Divulgación de Pruebas Electrónicas

Con la aprobación legislativa en segundo debate del expediente 24.783 y su posterior ratificación como Ley N.º 10778, publicada en La Gaceta N.º 198 de 22 de octubre de 2025, Costa Rica avanzó significativamente en la modernización de la cooperación internacional en materia penal cuando la evidencia es de naturaleza electrónica. La norma aprueba íntegramente el Segundo Protocolo Adicional al Convenio de Budapest (Consejo de Europa, 2022), que incorpora herramientas de obtención transfronteriza de datos con salvaguardas reforzadas de derechos fundamentales.

Mecanismos de cooperación

En cuanto a su operativización, el Protocolo habilita tres grandes vías de cooperación: cooperación directa con entidades privadas en el extranjero, asistencia acelerada

entre autoridades competentes y mecanismos específicos para situaciones de emergencia. Todo ello opera bajo principios de proporcionalidad y respeto a la privacidad.

Cooperación directa con entidades privadas

Entre las novedades más destacadas, el artículo 6 autoriza solicitar directamente a registradores de nombres de dominio (*registries*) en otro Estado información de registro con requisitos formales, estableciendo la obligación de designar una autoridad para canalizar estas consultas. Por su parte, el artículo 7 permite emitir órdenes directas a proveedores de servicios ubicados en otro país para obtener información específica de abonado, con posibilidad de formular reservas limitadas por razones de principios jurídicos internos.

Cooperación acelerada entre autoridades

Como refuerzo de la cooperación entre autoridades, el artículo 8 regula la producción expedita de información de abonado y datos de tráfico con plazos concretos: un plazo de hasta 20 días para información de abonado y de hasta 45 días para datos de tráfico. Además, establece requisitos de contenido y canales electrónicos seguros para las solicitudes. Estas obligaciones exigen que cada Estado parte designe autoridades emisoras y receptoras, y mantenga actualizados sus datos en el registro del Consejo de Europa.

Mecanismos de emergencia

En situaciones de emergencia con riesgo significativo e inminente para la vida o seguridad de personas, el artículo 9 permite solicitar la divulgación acelerada de datos almacenados a través de la Red 24/7 del Convenio, establecida en el artículo 35 del Convenio de Budapest, sin necesidad de pasar por los procedimientos ordinarios de asistencia jurídica mutua. Posteriormente, cada Estado parte debe cumplir con las formalidades que declare aplicables. Asimismo, el artículo 10 contempla mecanismos de asistencia jurídica mutua de emergencia y establece la obligación de mantener disponible personal de forma permanente en la autoridad central.

Implicaciones para Costa Rica

Este Protocolo consolida la posición de Costa Rica en el ámbito de la cooperación penal digital, otorgando herramientas operativas para formular solicitudes rápidas y directas de información. Sin embargo, también impone deberes de gobernanza, garantías procesales y coordinación interinstitucional que deben institucionalizarse a la brevedad para que la cooperación sea eficaz, legítima y respetuosa de los derechos fundamentales.

1.5. Decretos

1. Reglamento para la Protección de los Programas de Cómputo en los Ministerios e Instituciones Adscritas al Gobierno Central

El Reglamento para la Protección de los Programas de Cómputo en los Ministerios e Instituciones Adscritas al Gobierno Central, aprobado mediante Decreto Ejecutivo N.º 37549-JP (2012) y con reformas posteriores, constituye un marco normativo que procura asegurar el uso legal y responsable de los programas de cómputo en las entidades gubernamentales de Costa Rica. Este instrumento se enmarca en el conjunto de leyes nacionales e internacionales sobre derechos de autor y propiedad intelectual, reflejando el compromiso del Gobierno con el cumplimiento de los estándares de protección jurídica del *software* en el ámbito tecnológico.

Objeto y alcance

El Reglamento busca que las instituciones públicas prevengan y combatan el uso no autorizado de programas de cómputo, a fin de cumplir con lo establecido en materia de derechos de autor en la normativa nacional e internacional. Para ello, insta al establecimiento de sistemas y controles que permitan garantizar la utilización única y exclusiva de programas autorizados en todos los equipos y sistemas necesarios para el funcionamiento de cada institución.

Obligaciones institucionales

Las instituciones sujetas al Reglamento deben asegurar que la documentación de licencias se encuentre debidamente custodiada. Asimismo, deben mantener un registro constante de inventarios que incluya licencias de uso, instalaciones de *software* y demás autorizaciones correspondientes. Estas medidas tienen como finalidad garantizar el cumplimiento efectivo de la protección de derechos de autor en el ámbito gubernamental.

Cada Ministerio e institución adscrita al Gobierno Central tiene la obligación de realizar una auditoría anual que permita determinar el grado de cumplimiento con las disposiciones del Reglamento. En este sentido, deben presentar un informe ante el Registro Nacional de Derechos de Autor y Derechos Conexos indicando detalladamente el nivel de cumplimiento alcanzado, así como la cantidad de equipo disponible y las licencias correspondientes.

Supervisión y control

El Registro Nacional de Derechos de Autor y Derechos Conexos constituye el ente responsable de dar seguimiento al cumplimiento de lo establecido en el Reglamento mediante el análisis de los informes anuales presentados por las instituciones. En caso de detectar incongruencias o incumplimientos, debe escalar el informe a las autoridades pertinentes del Ministerio de Justicia y Paz para las acciones correctivas correspondientes.

2. Comisión Internet Costa Rica (CI-CR)

Creada en 2004 mediante el Decreto Ejecutivo N.º 32083 (2004) y adscrita al entonces Ministerio de Ciencia y Tecnología (hoy MICITT), la Comisión Internet Costa Rica (CI-CR) nace con el propósito de recomendar políticas y directrices estratégicas sobre el uso y desarrollo de Internet en Costa Rica. El decreto reconoce que la red trasciende fronteras y exige una visión global de política pública. Además, recuerda el papel del país en la administración del dominio de nivel superior de código de país (*country code Top-Level Domain*, ccTLD).cr a través de la Academia Nacional de Ciencias, conectando la gobernanza de dominios con el desarrollo de Internet.

Objetivos de la Comisión

El artículo 1 del Decreto formaliza la creación de la Comisión y su adscripción al MICITT. Por su parte, el artículo 2 fija como objetivo general canalizar y promover iniciativas públicas y privadas para el desarrollo de Internet en el país. El artículo 3 detalla los objetivos específicos, entre los cuales destaca el inciso c, que establece la promoción de estudios y la recomendación de procedimientos, normas técnicas y operacionales para asegurar el funcionamiento eficiente de redes y servicios de Internet, así como su uso creciente por parte de la sociedad.

Esta disposición se vincula directamente con la resiliencia y la seguridad digital, ya que sin estándares y procedimientos comunes no es posible garantizar la continuidad operativa ni la confianza en el ecosistema digital.

Composición y funcionamiento

El artículo 4 establece una composición multisectorial para la Comisión, integrada por representantes del MICITT (quien la preside), el Instituto Costarricense de Electricidad (ICE), la Cámara de Tecnologías de Información y Comunicación (CAMTIC), el Colegio de Profesionales en Computación e Informática y la Academia Nacional de Ciencias. El artículo 6 dispone que las sesiones deben realizarse al menos una vez cada dos meses para asegurar la continuidad de sus funciones.

Asimismo, el artículo 9 declara el desarrollo de Internet como tema de interés nacional, habilitando la posibilidad de recibir apoyo y colaboración de instituciones públicas para el cumplimiento de sus objetivos.

3. Directriz sobre Priorización de Soluciones de Cómputo en la Nube en el Sector Público

La Directriz N.º 046-H-MICITT (2013), vigente desde el 16 de mayo de 2013, instruye al sector público a priorizar servicios de cómputo en la nube frente a otras infraestructuras cuando resulte técnica y financieramente viable, como parte de la estrategia de modernización del Estado. El mandato cubre equipos, licencias, sistemas operativos y ofimáticos, correo electrónico, hospedaje web, aplicaciones, bases de datos, cortafuegos y demás componentes tecnológicos, tanto para usuario final como para centros de datos.

Importa resaltar que el artículo 2 exige que toda adquisición de infraestructura TIC incluya una evaluación comparativa con opciones de cómputo en la nube en tres dimensiones. En el plano técnico, debe analizarse la funcionalidad, integración, disponibilidad, soporte, confidencialidad y seguridad de la información, así como los requerimientos de capacitación. En los planos legal y financiero, debe calcularse el valor presente de todos los costos proyectados a tres años.

Si tras el análisis la institución decide no optar por servicios en la nube, debe garantizar la misma calidad de servicio mediante acuerdos de nivel de servicio (SLA, *Service Level Agreement*) internos medibles, con penalidades por incumplimiento equivalentes a los que exigiría a un proveedor externo de servicios en la nube.

Ámbito de aplicación ampliado

Aunque la Directriz vincula directamente a las instituciones de la Administración Central sujetas a jerarquía del Poder Ejecutivo, también insta a los Supremos Poderes, las universidades estatales, las municipalidades, la Caja Costarricense de Seguro Social (CCSS) y demás entes autónomos a aplicar los artículos 1 y 2, en concordancia con la política de contención del gasto público. De esta manera, el instrumento busca una coordinación nacional en materia de infraestructura tecnológica.

Gobernanza y trazabilidad

En materia de gobernanza y trazabilidad, los jerarcas de cada entidad son responsables de dos obligaciones principales. Primero, deben emitir un informe técnico anual con el seguimiento dado a la Directriz, el cual debe remitirse al Consejo Presidencial de Competitividad e Innovación. Segundo, deben informar de manera

continua al Viceministerio de Telecomunicaciones sobre sus proyectos de TIC y gobierno digital.

Esta segunda obligación busca mantener un registro central que evite inversiones redundantes y permita dar seguimiento efectivo a las iniciativas tecnológicas del sector público. Para ello, se contempla la creación de un instrumento, preferiblemente en línea, para capturar, clasificar y agrupar datos relevantes de los proyectos. En todo caso, la información registrada no debe exponer detalles que comprometan la seguridad de la información ni la infraestructura tecnológica institucional.

4. Directriz N.° 036-MTSS-MICITT sobre Implementación de Accesibilidad en Sitios Web del Sector Público

La Directriz N.° 036-MTSS-MICITT (2024), emitida el 16 de enero de 2024, renueva la política pública de accesibilidad digital en el Estado y deroga la Directriz N.° 051-MTSS-MICITT (2019). Esta normativa tiene como finalidad ordenar a la Administración Pública Central la implementación de accesibilidad en sus sitios web e instar al resto del sector público a adoptar el mismo estándar. El objetivo es garantizar que todas las personas, incluidas las personas con discapacidad, accedan en igualdad de condiciones a la información y los servicios públicos en línea.

Estándar técnico y plazos de cumplimiento

La Directriz adopta como estándar técnico las Pautas de Accesibilidad para el Contenido Web (*Web Content Accessibility Guidelines*, WCAG por sus siglas en inglés) 2.1 y fija plazos específicos para su cumplimiento. Las instituciones deben alcanzar el Nivel A en un plazo máximo de tres años desde la vigencia de la Directriz y el Nivel AA en un plazo de seis años. El Nivel AAA se considera recomendable, pero no obligatorio.

Implementación y supervisión

La Directriz instruye al MICITT y al Consejo Nacional de Personas con Discapacidad (CONAPDIS) a emitir y comunicar los lineamientos técnicos requeridos a las instituciones públicas de la Administración Pública Central y la Administración Pública Descentralizada. Las instituciones estarán sujetas a un proceso de verificación por parte de CONAPDIS, que, además, deberá publicar anualmente un informe nacional sobre el estado de accesibilidad de los sitios web públicos.

Obligaciones operativas y transparencia

Para su implementación, la Directriz establece que el desarrollo y mantenimiento de los sitios web, incluidos aquellos que provengan de donaciones, deben cumplir los

requisitos de accesibilidad establecidos. Asimismo, dispone que cada portal debe incluir información clara sobre el nivel de accesibilidad alcanzado y la fecha de la última revisión. Además, los sitios deben contar con un mecanismo de contacto accesible que permita a las personas usuarias reportar dificultades de acceso o sugerir mejoras.

5. Decreto Ejecutivo N.° 44196-MSP-MICITT - Reglamento sobre Medidas de Ciberseguridad Aplicables a los Servicios de Telecomunicaciones Basados en Tecnología 5G y Superiores

El Decreto Ejecutivo N.° 44196-MSP-MICITT (2023) introduce el Reglamento sobre Medidas de Ciberseguridad para Servicios de Telecomunicaciones que emplean tecnología móvil de quinta generación (5G) y superiores. El propósito principal de este Reglamento es garantizar el uso y explotación seguros de estas redes y servicios, protegiendo la privacidad de los usuarios.

Ámbito de aplicación

El Reglamento es aplicable a toda entidad pública o privada, nacional o extranjera, que ofrezca servicios de telecomunicaciones basados en tecnología 5G en el territorio nacional. Quedan excluidas de su ámbito las redes privadas de telecomunicaciones.

Riesgos identificados

Para asegurar un uso eficiente y seguro de las redes 5G y servicios de telecomunicaciones relacionados, el Reglamento identifica y aborda varios riesgos nacionales de ciberseguridad. Estos riesgos incluyen la seguridad ineficiente de las infraestructuras, las vulnerabilidades en las cadenas de suministro de la tecnología 5G, las operaciones de actores maliciosos, las interdependencias entre redes 5G y los riesgos asociados con dispositivos de usuarios finales.

Obligaciones en materia de estándares

En respuesta a estos riesgos, el Reglamento establece la obligación de adoptar estándares internacionales sobre ciberseguridad, específicamente las normas ISO/IEC 27001:2022, ISO/IEC 27002:2022, ISO/IEC 27003:2017, ISO/IEC 27011:2016 y la norma SCS 9001. Estos estándares abarcan la protección de la privacidad, controles de seguridad y técnicas para la gestión de riesgos de seguridad de la información.

Análisis de riesgos y medidas de gestión

Las entidades sujetas a este Reglamento deben realizar análisis de riesgo de ciberseguridad en sus redes, centrándose en la detección de vulnerabilidades y amenazas. Tras estas evaluaciones, deben adoptar medidas adecuadas para gestionar los riesgos identificados. Además, deben prestar especial atención a la protección de la seguridad nacional y al resguardo del derecho a la intimidad, privacidad y secreto de las comunicaciones.

Aspectos controvertidos del Reglamento

El Reglamento presenta aspectos que generan interrogantes desde la perspectiva técnica y normativa. En particular, establece restricciones para la utilización de equipos de empresas cuya sede se ubica en países que no se han adherido al Convenio de Budapest sobre Ciberdelincuencia (2001) en elementos críticos de la red 5G, bajo el argumento de que representan un alto riesgo de ciberseguridad.

Esta disposición plantea tensiones con el principio de neutralidad tecnológica, reconocido en la normativa nacional y en tratados internacionales suscritos por Costa Rica. Dicho principio garantiza que los operadores de redes y proveedores de servicios de telecomunicaciones puedan elegir libremente sus tecnologías, siempre que cumplan con estándares de seguridad técnicos establecidos en las especificaciones de las licitaciones y contratos.

La controversia radica en que el Convenio de Budapest constituye fundamentalmente un marco de cooperación penal internacional para la persecución de delitos cibernéticos, que exige a los Estados parte establecer una base común de tipos penales en sus legislaciones nacionales. Sin embargo, no constituye en sí mismo un estándar técnico de ciberseguridad, lo que genera dudas sobre la pertinencia de su utilización como criterio para evaluar el nivel de riesgo de equipamiento tecnológico en infraestructuras críticas de telecomunicaciones.

Esta aproximación podría interpretarse como una restricción comercial que no se fundamenta directamente en criterios técnicos de seguridad verificables mediante auditorías o certificaciones de las normas ISO/IEC mencionadas en el propio Reglamento, sino en la pertenencia o no a un tratado de naturaleza penal-procesal.

Control de constitucionalidad

Esta regulación ha sido objeto de control constitucional. Se pueden identificar dos acciones de inconstitucionalidad que fueron declaradas inadmisibles sin estudio de

fondo: Sala Constitucional de Costa Rica, Sentencia 2023-030482 (22 de noviembre de 2023) y Sentencia 2024-003226 (7 de febrero de 2024).

Una tercera acción de inconstitucionalidad (expediente 24-024405-0007-CO) fue admitida para estudio de fondo el 4 de diciembre de 2024. Esta acción cuestiona diversos aspectos del Reglamento, específicamente los artículos 6, 8 inciso i, 9 y 10. Los cuestionamientos incluyen:

I. La imposición del estándar SCS 9001 y otros estándares específicos.
II. La diversificación obligatoria de proveedores.
III. Los parámetros de alto riesgo establecidos en los incisos c a f, que incluyen la adhesión al Convenio de Budapest como factor determinante.

Los alegatos de inconstitucionalidad se fundamentan en posibles afectaciones al principio de reserva de ley, la separación de poderes, la igualdad y no discriminación, las libertades económicas, la neutralidad tecnológica y la proporcionalidad. Asimismo, se plantean eventuales tensiones con compromisos comerciales internacionales asumidos por Costa Rica.

Procesalmente, la Sala Constitucional confirió audiencia a la Procuraduría General de la República y a los ministerios competentes. Además, dejó claro que la admisión a trámite no suspende la vigencia general del Decreto, el cual continúa rigiendo mientras se resuelve el fondo del asunto. No obstante, podrían producirse efectos en casos concretos según las reglas de la jurisdicción constitucional.

¿Qué dijo la Sala Constitucional?

Sobre lo indicado, la Sala Constitucional ha reconocido un margen de configuración estatal para establecer regulaciones en materia de ciberseguridad, siempre que no lesionen derechos fundamentales. De igual forma, ha encauzado las controversias de naturaleza estrictamente técnica hacia la jurisdicción ordinaria.

El debate sobre la neutralidad tecnológica y el uso del Convenio de Budapest como criterio de elegibilidad de proveedores evidencia tensiones entre objetivos de seguridad nacional, competencia económica e innovación tecnológica. Si bien el estándar constitucional permite al Poder Ejecutivo elevar exigencias por razones de ciberseguridad, a nivel operativo resulta conveniente que las entidades sustenten cada restricción en análisis técnicos proporcionales y auditables.

Para garantizar la legitimidad y eficacia de las medidas, la adopción de controles debería basarse en estándares técnicos internacionalmente aceptados y en evaluaciones de riesgo concretas del entorno tecnológico 5G costarricense. Esta

aproximación permitiría conciliar los objetivos de seguridad con los principios de proporcionalidad, no discriminación y neutralidad tecnológica que rigen el sector de las telecomunicaciones.

6. Decreto Ejecutivo N.º 45061-MICITT - Reglamento para la Gobernanza en Ciberseguridad y la Resiliencia Cibernética de las Instituciones Gubernamentales

El Decreto Ejecutivo N.º 45061-MICITT (2025), publicado el 16 de junio de 2025, establece el Reglamento para la Gobernanza en Ciberseguridad y la Resiliencia Cibernética de las Instituciones Gubernamentales y deroga el Decreto Ejecutivo N.º 37052-MICIT (2012) que originalmente creó el Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR). Este instrumento normativo representa una modernización integral del marco institucional de ciberseguridad del Estado costarricense, surgida como respuesta a los ciberataques de 2022 y alineada con la Estrategia Nacional de Ciberseguridad 2023-2027.

Objeto y ámbito de aplicación

El Reglamento tiene por objeto establecer el marco de gobernanza en materia de ciberseguridad y definir las condiciones para gestionar la resiliencia cibernética de la Administración Central. De igual forma, busca colaborar con los demás Poderes del Estado y la Administración Descentralizada, con el fin de fortalecer integralmente la ciberseguridad nacional.

El Decreto define conceptos fundamentales para su aplicación. La resiliencia cibernética se entiende como la capacidad de una organización para anticiparse, resistir, responder y recuperarse eficazmente de incidentes cibernéticos, asegurando la continuidad operativa y minimizando el impacto negativo sobre sus activos digitales y procesos críticos. Por su parte, la gobernanza de ciberseguridad comprende el conjunto de procesos, políticas, estructuras organizativas y mecanismos establecidos para dirigir, controlar y evaluar la gestión de la ciberseguridad dentro de una organización.

Fortalecimiento de la rectoría del MICITT

El artículo 3 reafirma la condición del MICITT como órgano rector en materia de ciencia, innovación, tecnología y telecomunicaciones. En este rol, el MICITT puede coordinar con los Poderes del Estado y la Administración Descentralizada que gestionan sistemas de información o servicios tecnológicos esenciales, en temas de desarrollo e implementación de políticas públicas, marcos normativos, estándares técnicos y procedimientos de ciberseguridad.

Creación de la Dirección de Ciberseguridad

El Reglamento crea formalmente la Dirección de Ciberseguridad (DC) del MICITT, estableciéndola como la dependencia designada para liderar y coordinar a nivel nacional, con los poderes del Estado, instituciones autónomas, empresas y bancos estatales, todo lo relacionado con la seguridad informática y cibernética. La DC tiene por objetivo fortalecer la resiliencia y seguridad de la infraestructura digital del país.

Entre las funciones asignadas a la DC se encuentran: promover políticas y estrategias nacionales de ciberseguridad, fungir como punto central de coordinación en la respuesta a incidentes, liderar iniciativas de capacitación, proporcionar asesoramiento a organizaciones gubernamentales, coordinar la evaluación de riesgos a nivel nacional, dirigir investigaciones sobre amenazas emergentes, emitir criterio técnico basado en evidencia, colaborar con agencias internacionales y realizar alianzas estratégicas para el fortalecimiento del ecosistema de ciberseguridad.

Modelo de gestión basado en estándares internacionales

El artículo 6 establece que el modelo de gestión de la DC se fundamenta en estándares internacionales reconocidos, particularmente el Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología versión 2.0 (NIST CSF 2.0). El modelo incorpora las siguientes funciones esenciales del ciclo de ciberseguridad: gobernanza, identificación, protección, detección, respuesta y recuperación.

La DC debe identificar, administrar y mitigar los riesgos asociados a sus funciones estratégicas y operativas mediante planes de gestión de riesgos, continuidad operativa y controles compensatorios. De igual forma, el MICITT promoverá que todas las instituciones de la Administración Pública adopten e implementen sus propios planes institucionales de gestión de riesgos cibernéticos, siguiendo metodologías armonizadas y controles mínimos esenciales.

Estructura organizativa: CSIRT-CR y SOC-CR

Para el cumplimiento de sus fines estratégicos, operativos y técnicos, la Dirección de Ciberseguridad cuenta con dos departamentos especializados: el Departamento Centro de Respuesta a Incidentes de Ciberseguridad (CSIRT-CR) y el Departamento Centro de Operaciones de Ciberseguridad (SOC-CR).

El CSIRT-CR tiene como objetivo responder a incidentes de ciberseguridad que afecten a las instituciones de gobierno y operadores de infraestructura crítica. Entre sus funciones se encuentran: ejecutar acciones de respuesta ante incidentes cibernéticos, coordinar acciones interinstitucionales e internacionales, proporcionar

orientación técnica en el diseño de políticas, promover la implementación de iniciativas en ciberseguridad, elaborar informes de incidentes, realizar análisis de ciberinteligencia y análisis forense post incidente, generar alertas tempranas y asesorar en la respuesta a incidentes.

Por su parte, el SOC-CR tiene como objetivo proteger y monitorear las infraestructuras críticas de las instituciones públicas definidas por el MICITT. Sus funciones incluyen: realizar monitoreo continuo 24/7 de redes y sistemas, proteger en tiempo real las plataformas tecnológicas, elaborar informes periódicos de monitoreo, analizar eventos de ciberseguridad, apoyar al CSIRT-CR con información sobre amenazas detectadas, realizar análisis de vulnerabilidades, velar por el cumplimiento de estándares de seguridad y definir soluciones de seguridad avanzada para el monitoreo y detección de ciberataques.

Obligaciones de las instituciones gubernamentales

El artículo 12 establece obligaciones específicas para las personas jerarcas de la Administración Central en el marco del fortalecimiento de la resiliencia cibernética del Estado. Estas obligaciones comprenden:

I. Adoptar e implementar medidas de gobernanza en ciberseguridad, incluyendo la designación de responsables institucionales, elaboración de políticas internas, planes de gestión de riesgos cibernéticos, continuidad operativa y recuperación ante incidentes.
II. Aplicar los lineamientos técnicos, protocolos, estándares y procedimientos que emita el MICITT en materia de ciberseguridad, asegurando su incorporación en los procesos institucionales.
III. Cumplir con las medidas técnicas emitidas por la DC orientadas a mejorar las capacidades de prevención, detección, respuesta y recuperación ante ciberamenazas.
IV. Brindar de manera oportuna y veraz la información requerida por la DC cuando esté relacionada con evaluación de riesgos, incidentes, capacidades tecnológicas o cumplimiento normativo.
V. Reportar de forma obligatoria, dentro de un plazo máximo de veinticuatro horas, cualquier incidente de ciberseguridad que comprometa la disponibilidad, integridad, confidencialidad o autenticidad de los sistemas tecnológicos, redes, plataformas digitales o servicios institucionales.
VI. Colaborar activamente con los procesos de respuesta y mitigación de incidentes, incluyendo la conformación de equipos técnicos institucionales especializados.
VII. Facilitar el acceso a personal técnico autorizado a los entornos tecnológicos pertinentes cuando se requiera para la ejecución de medidas urgentes de contención o análisis forense, respetando el marco legal vigente en materia de protección de datos y derechos fundamentales.

Sistema de reporte de incidentes

El artículo 14 refuerza la obligación de reporte de incidentes de ciberseguridad al CSIRT-CR. El reporte debe realizarse en un plazo no mayor a veinticuatro horas desde la detección del incidente, a través del instrumento oficial habilitado por el CSIRT-CR, incluyendo al menos una descripción preliminar del evento, sistemas afectados, medidas adoptadas y datos de contacto técnico.

La DC puede establecer niveles de criticidad y priorización para incidentes reportados, conforme a una clasificación estandarizada que incluye categorías crítico, alto, medio y bajo. Las instituciones deben colaborar activamente en la investigación, contención y mitigación de los incidentes, siguiendo las instrucciones técnicas del CSIRT-CR.

Modelo de evaluación de madurez cibernética

El artículo 15 establece que la DC implementará un modelo de evaluación de madurez cibernética que incluirá al menos: el nivel de adopción de políticas y controles de ciberseguridad, las capacidades técnicas y humanas instaladas, y la existencia de planes de continuidad, respuesta a incidentes y resiliencia operativa.

Los resultados permitirán clasificar a las instituciones en niveles de madurez básico, intermedio o avanzado, y establecer prioridades de inversión, capacitación y asistencia técnica. La participación en el modelo nacional de madurez cibernética es de acatamiento obligatorio para la Administración Pública Central y sus órganos con desconcentración mínima o máxima.

Declaratoria de interés público

El artículo 13 declara de interés público todas las acciones y proyectos institucionales orientados al fortalecimiento de la ciberseguridad, la resiliencia cibernética y la protección de la infraestructura digital del país, tanto en el ámbito público como privado. Esta declaratoria autoriza a las entidades públicas y privadas a apoyar las labores del MICITT en materia de ciberseguridad mediante la participación en mesas técnicas, el intercambio responsable de información técnica, el desarrollo conjunto de investigaciones y tecnologías, y el apoyo a programas de capacitación y fortalecimiento institucional.

Implicaciones para el ecosistema de ciberseguridad nacional

Este Decreto representa un avance sustancial en la institucionalización de la ciberseguridad en Costa Rica. La transición del CSIRT-CR de un centro de respuesta

reactivo a una Dirección de Ciberseguridad integral con capacidades de monitoreo continuo (SOC-CR) refleja la evolución hacia un modelo proactivo de gestión de riesgos cibernéticos.

Además, la adopción del marco NIST CSF 2.0 como modelo de gestión alinea a Costa Rica con las mejores prácticas internacionales y facilita la interoperabilidad con otros países en materia de cooperación en ciberseguridad. Asimismo, el establecimiento de obligaciones claras de reporte y colaboración para las instituciones gubernamentales crea un ecosistema de responsabilidad compartida en la protección de la infraestructura digital del Estado.

Sin embargo, la efectividad del Reglamento dependerá de la capacidad de las instituciones para cumplir con las obligaciones establecidas, particularmente aquellas con menores recursos técnicos y financieros. El modelo de evaluación de madurez cibernética permitirá identificar brechas y priorizar el fortalecimiento institucional, pero requerirá inversión sostenida y desarrollo de capacidades humanas especializadas en el mediano y largo plazo.

7. Decreto Ejecutivo N.° 40199-MP - Apertura de Datos Públicos

El Decreto Ejecutivo N.° 40199-MP (2017) establece la apertura de datos como política de Estado en Costa Rica. Su objetivo es disponer que los datos de carácter público se pongan a disposición como datos abiertos para facilitar su acceso, uso, reutilización y redistribución con cualquier fin lícito.

Definiciones y principios

La norma define dato abierto como aquel disponible en línea, sin procesar, en formato abierto, neutral e interoperable, descargable completo, sin costo ni registro y procesable por computadora. Asimismo, establece principios operativos fundamentales: abiertos por defecto, oportunos y exhaustivos, accesibles y utilizables, comparables, neutrales e interoperables.

En la práctica, esto implica que la apertura debe considerarse desde la etapa en que se genera el dato, y no como un esfuerzo residual o posterior a su creación. Este enfoque busca incorporar la cultura de datos abiertos en el diseño mismo de los sistemas de información gubernamentales.

Ámbito de aplicación

El Decreto es obligatorio para la Administración Pública Central. Como instrumento de política pública, establece lineamientos y una guía para estandarizar la práctica

institucional, que otras entidades pueden tomar como marco de referencia para sus propios procesos de apertura de datos.

Estructura de gobernanza

La estructura de gobernanza se organiza en tres instancias. La Comisión Nacional de Datos Abiertos actúa como órgano rector de la política. La Secretaría Técnica ejerce funciones de coordinación ejecutiva. El Grupo de Enlaces Institucionales vincula la apertura de datos con las prioridades y capacidades de cada institución. Estas tres instancias son responsables de coordinar la ejecución de la política, armonizar conjuntos de datos y garantizar la alineación con los objetivos estratégicos del Estado. Proceso de apertura de datos

El Decreto establece un proceso estructurado y auditable para la apertura de datos que comprende las siguientes etapas: identificación de demanda ciudadana e institucional, evaluación del estado de la información disponible, priorización de conjuntos de datos según criterios de impacto y viabilidad, limpieza y estandarización de datos, análisis de confidencialidad y protección de datos personales, generación de metadatos descriptivos, selección de formatos abiertos apropiados, aplicación de licenciamiento adecuado, publicación en plataformas accesibles y comunicación a usuarios potenciales.

Toda institución sujeta al Decreto debe publicar su catálogo de datos abiertos en el portal nacional *datosabiertos.presidencia.go.cr*, sin perjuicio de difundir la información también en sus propios sitios web institucionales. Esta centralización busca facilitar el acceso ciudadano y garantizar la interoperabilidad entre conjuntos de datos de diferentes instituciones.

Protección de datos personales y confidencialidad

El Decreto establece salvaguardas específicas para la protección de datos personales en el contexto de la apertura de datos públicos. Para publicar información en formato abierto, las instituciones deben omitir datos personales protegidos por la legislación vigente, particularmente aquellos regulados por la Ley N.º 8968 (2011) de Protección de la Persona Frente al Tratamiento de sus Datos Personales.

Además, deben aplicarse técnicas de anonimización que garanticen la no reidentificación posterior de personas físicas o jurídicas cuando los conjuntos de datos contengan información sensible. Esta disposición busca equilibrar el derecho de acceso a la información pública con el derecho fundamental a la protección de datos personales.

Mecanismo de solicitud ciudadana

El Decreto establece un mecanismo mediante el cual cualquier persona puede solicitar la liberación de conjuntos de datos específicos. La institución receptora de la solicitud debe responder en un plazo de entre diez y treinta días hábiles, dependiendo de la complejidad de la solicitud y la disponibilidad de la información.

La respuesta institucional puede consistir en la publicación del conjunto de datos solicitado en el portal nacional, o bien en una denegatoria fundamentada con base legal que justifique las razones por las cuales la información no puede publicarse en formato abierto. Esta última situación puede presentarse cuando existan restricciones legales relacionadas con seguridad nacional, protección de datos personales, secretos comerciales o industriales, o información en proceso de toma de decisiones.

Implicaciones para la transparencia y la innovación

Este Decreto representa un avance significativo en la institucionalización de la transparencia y el acceso a la información pública en Costa Rica. La política de datos abiertos no solo fortalece la rendición de cuentas gubernamental, sino que también habilita la generación de valor económico y social mediante la reutilización de datos públicos por parte de emprendedores, investigadores, organizaciones de la sociedad civil y el sector privado.

La estandarización de formatos y la adopción de principios de interoperabilidad facilitan el desarrollo de aplicaciones, servicios y análisis basados en datos gubernamentales, contribuyendo a la economía digital y la innovación tecnológica. Sin embargo, la efectividad de esta política dependerá de la capacidad institucional para generar datos de calidad, mantener actualizada la información publicada y responder adecuadamente a las solicitudes ciudadanas.

8. Decreto Ejecutivo N.° 44487-MICITT - Lineamientos para la Implementación del Proyecto de Fortalecimiento de las Capacidades en Ciberseguridad del País

El Decreto Ejecutivo N.° 44487-MICITT (2024), vigente desde el 13 de junio de 2024, oficializa los lineamientos que habilitan al MICITT para recibir, asignar y distribuir recursos donados por el Gobierno de los Estados Unidos con el fin de fortalecer las capacidades en ciberseguridad de las instituciones públicas. El instrumento se enmarca en el contexto del estado de emergencia declarado por los ciberataques de 2022 (Decreto Ejecutivo N.° 43542-MP-MICITT) y la Directriz N.° 133-MP-MICITT, que reconocen la necesidad de elevar las capacidades técnicas y de gestión en todo el sector público costarricense.

Objeto y alcance del Decreto

El artículo 1 formaliza los lineamientos y precisa su propósito operativo, estableciendo que estas disposiciones del MICITT ordenan la recepción, asignación y distribución de la donación para fortalecer capacidades de ciberseguridad del Estado. La prioridad se establece en soluciones de Centro de Operaciones de Seguridad (SOC), monitoreo continuo y administración centralizada de seguridad.

Lineamientos técnicos y administrativos

El Decreto incorpora un conjunto de lineamientos técnicos y administrativos que regulan la implementación del proyecto de fortalecimiento.

Financiamiento y alcance del proyecto

El proyecto se financia mediante una donación equivalente a veinticinco millones de dólares estadounidenses (USD 25 millones), ejecutada por una fundación estadounidense. Los recursos se destinan a la adquisición de equipo especializado, la implementación de servicios de SOC de forma temporal y la contratación de servicios de detección y respuesta gestionadas (MDR, *Managed Detection and Response*). El objetivo es dotar a las instituciones públicas de capacidades para monitorear, detectar, prevenir y atender incidentes de ciberseguridad de manera proactiva y coordinada.

Competencia y rol del CSIRT-CR

El MICITT, a través del Centro de Respuesta a Incidentes de Ciberseguridad (CSIRT-CR), ejerce las funciones de aprobación de donaciones específicas, supervisión de la ejecución del proyecto y evaluación de resultados. El CSIRT-CR actúa como instancia técnica de seguimiento, garantizando que la implementación de las soluciones se alinee con los objetivos estratégicos de ciberseguridad nacional y los estándares técnicos establecidos.

Selección de instituciones beneficiarias

El CSIRT-CR es responsable de definir las instituciones públicas que se priorizan como beneficiarias del proyecto. La selección inicia con los dieciocho ministerios del Poder Ejecutivo y se extiende progresivamente a instituciones que gestionan infraestructura crítica y servicios esenciales del Estado. Este criterio de priorización reconoce que ciertos actores estatales tienen mayor exposición a amenazas cibernéticas debido a la naturaleza estratégica de los servicios que prestan.
Obligaciones de las instituciones beneficiarias

Cada institución beneficiaria debe cumplir con un conjunto de obligaciones específicas. En primer lugar, debe conformar un equipo profesional especializado en ciberseguridad y designar un punto de contacto técnico que coordine con el CSIRT-CR. De igual forma debe facilitar la realización de diagnósticos de seguridad, coordinar las actividades de instalación de equipos y configuración de servicios, y mantener inventarios y registros actualizados de equipos, licencias, capacitaciones recibidas y servicios implementados.

Una obligación particularmente relevante es la planificación presupuestaria que las instituciones deben realizar desde el año 2025 para garantizar la sostenibilidad de las protecciones implementadas a partir de 2026. Esto incluye la provisión de recursos para actualizaciones de *software*, renovación de licencias y continuidad de servicios de monitoreo y respuesta. Esta disposición reconoce que la donación inicial es un impulso temporal y que la responsabilidad de largo plazo recae en cada institución beneficiaria.

Formalización y patrimonio

El Decreto establece que las donaciones se materializan mediante convenios interinstitucionales entre el MICITT y cada institución beneficiaria. Los bienes y equipos adquiridos pasan a formar parte del patrimonio de cada institución receptora, la cual debe identificarlos y controlarlos conforme al ordenamiento jurídico vigente en materia de administración de bienes públicos.

Obligatoriedad, actualización y vigencia

El artículo 2 declara de acatamiento obligatorio estos lineamientos para todas las instituciones públicas seleccionadas como beneficiarias del proyecto. El artículo 3 encarga al MICITT mantener los lineamientos actualizados y disponibles públicamente en su sitio web institucional, garantizando la transparencia y el acceso a la información sobre la implementación del proyecto. El artículo 4 establece que la vigencia del Decreto se extiende hasta la finalización formal del proyecto de fortalecimiento.
Implicaciones para la arquitectura nacional de ciberseguridad

Este Decreto representa un hito significativo en el fortalecimiento de la arquitectura nacional de ciberseguridad de Costa Rica. La incorporación de servicios de SOC y MDR en instituciones públicas marca una transición del modelo reactivo de respuesta a incidentes hacia un modelo proactivo de monitoreo continuo, detección temprana y respuesta coordinada.

La implementación de estas capacidades permitirá generar información empírica sobre la efectividad de las medidas de protección, la reducción de tiempos

de detección y respuesta, y la disminución de la exposición a amenazas en las instituciones beneficiadas. Esta información resultará fundamental para evaluar el impacto del proyecto y justificar la asignación de recursos permanentes para sostener estas capacidades más allá del período de donación.

Sin embargo, el éxito del proyecto dependerá críticamente de la capacidad de las instituciones para cumplir con su obligación de planificación presupuestaria y sostenibilidad. La experiencia internacional muestra que proyectos de fortalecimiento basados en donaciones enfrentan riesgos de discontinuidad una vez que finaliza el apoyo externo. El requisito de planificación desde 2025 busca mitigar este riesgo, pero su efectividad dependerá de la disponibilidad presupuestaria real y la priorización que cada institución asigne a la ciberseguridad en un contexto de restricciones fiscales.

Además, la concentración inicial en los dieciocho ministerios del Poder Ejecutivo, aunque estratégicamente justificada, deja temporalmente desprotegidas otras entidades del sector público que también gestionan información sensible y servicios críticos. La expansión progresiva del proyecto a instituciones autónomas, municipalidades y otras entidades descentralizadas requerirá recursos adicionales y mecanismos de priorización que equilibren criterios de riesgo, impacto y viabilidad técnica.

9. Código Nacional de Tecnologías Digitales - Decreto Ejecutivo N.° 44507-MICITT

El Código Nacional de Tecnologías Digitales (CNTD), aprobado mediante el Decreto Ejecutivo N.° 44507-MICITT (2024), constituye un instrumento normativo fundamental del MICITT para ordenar la transformación digital del Estado costarricense. Su propósito es establecer estándares y buenas prácticas que deben seguir las instituciones públicas cuando adquieren, desarrollan y operan tecnologías, con el fin de garantizar servicios eficientes, accesibles y centrados en la persona usuaria.

Ámbito de aplicación

La aplicación del CNTD es obligatoria para todo el sector público que impulse iniciativas con componente digital. Se exceptúan de su aplicación únicamente los ámbitos de defensa nacional y seguridad del Estado, dada la naturaleza sensible de estos sectores. Esta obligatoriedad busca asegurar la uniformidad, interoperabilidad y coherencia en la prestación de servicios digitales a lo largo de toda la Administración Pública.

Principios rectores

El Código se fundamenta en un principio transversal de democratización tecnológica, estableciendo que la digitalización debe beneficiar de forma equitativa a toda la población. En consecuencia, incorpora lineamientos de accesibilidad universal, enfoque inclusivo, transparencia y participación ciudadana. Estos principios buscan que cada proyecto tecnológico mejore no solo la eficiencia interna de las instituciones, sino también la confianza ciudadana y el control social sobre la gestión pública.

Rol del MICITT como órgano rector

Como órgano rector en materia de tecnologías digitales, el MICITT conduce la implementación del Código, difunde sus contenidos y lo actualiza periódicamente conforme evolucionen las tecnologías y las necesidades del sector público. Asimismo, acompaña técnicamente a las instituciones en su adopción, impulsa programas de capacitación continua y supervisa su aplicación efectiva.

Ámbitos de aplicación del Código

El CNTD cubre todo el ciclo de vida de los proyectos tecnológicos gubernamentales. Abarca desde la planificación estratégica y el diseño de arquitecturas empresariales hasta la adquisición de soluciones, el desarrollo de sistemas, la integración con plataformas existentes, la operación de servicios y el mantenimiento de infraestructuras.

En cada una de estas etapas, el Código incorpora criterios específicos de gestión de riesgos, seguridad de la información, gobernanza e interoperabilidad de datos, accesibilidad, continuidad operativa y evaluación de impacto. Esta aproximación integral busca que las consideraciones de seguridad, privacidad y calidad no sean agregadas posteriormente, sino que se integren desde el diseño mismo de cada solución tecnológica.

Estandarización y control

El CNTD estructura la transformación digital en un proceso reglado, medible y sostenible. Genera un lenguaje técnico común para toda la Administración Pública, lo que facilita la comunicación entre instituciones y la reutilización de soluciones. Establece exigencias claras que deben incorporarse en los carteles de licitación y en los contratos de adquisición de tecnología, garantizando que los proveedores cumplan con estándares mínimos de calidad, seguridad e interoperabilidad.

Asimismo, proporciona una ruta metodológica para que cada inversión tecnológica se traduzca en valor público tangible, mediante indicadores de desempeño, mecanismos de

evaluación y requisitos de documentación que permiten dar seguimiento al retorno de la inversión y al impacto ciudadano de los proyectos.

Implicaciones para la gobernanza tecnológica

La adopción del CNTD como marco normativo obligatorio representa un avance significativo en la gobernanza tecnológica del Estado costarricense. Al establecer requisitos comunes y verificables, reduce la heterogeneidad en la calidad de las soluciones digitales públicas y facilita la interoperabilidad entre sistemas de diferentes instituciones.

Sin embargo, la efectividad del Código enfrenta varios desafíos de implementación. En primer lugar, las instituciones presentan diferentes niveles de madurez digital y capacidad técnica. Aquellas con equipos especializados y recursos suficientes pueden adoptar los estándares del CNTD con relativa facilidad, mientras que instituciones más pequeñas o con menor presupuesto tecnológico enfrentan barreras significativas.

En segundo lugar, la supervisión efectiva del cumplimiento requiere que el MICITT cuente con capacidades de auditoría técnica y recursos para proporcionar asistencia a las instituciones. El acompañamiento técnico mencionado en el Decreto implica una inversión sostenida en equipos especializados que puedan realizar evaluaciones de conformidad, emitir dictámenes técnicos y orientar procesos de mejora.

Finalmente, la actualización periódica del Código resulta fundamental dado el ritmo acelerado de evolución tecnológica. Un marco normativo que no se actualice regularmente corre el riesgo de convertirse en obsoleto o de establecer barreras innecesarias a la adopción de nuevas tecnologías. El equilibrio entre estabilidad normativa y flexibilidad para incorporar innovaciones constituye un desafío permanente para el MICITT como ente rector.

10. Directriz N.° 053-H-MICITT (2019) - Regulación y Normalización de Adquisiciones de Tecnología y Desarrollo de Sistemas Informáticos de Apoyo a la Gestión

La Directriz N.° 053-H-MICITT (2019), emitida conjuntamente por el Ministerio de Hacienda y el MICITT, busca ordenar cómo el Estado adquiere tecnología y desarrolla sistemas para la gestión pública. Su propósito se centra en dos aspectos fundamentales: la eficiencia y transparencia en el uso de los recursos públicos, y la estandarización de criterios técnicos para que las inversiones tecnológicas mejoren efectivamente la operación institucional y el servicio a la ciudadanía.
Ámbito de aplicación

El alcance de la Directriz comprende tanto la Administración Pública Central como la Descentralizada. Las entidades sujetas a su aplicación deben ajustarse a las Normas Técnicas de la Contraloría General de la República y a los lineamientos del MICITT en todo el ciclo de vida de las tecnologías: planeación, contratación, implementación y mantenimiento de equipos y sistemas informáticos.

Procedimientos de contratación

La Directriz establece que los procedimientos de contratación administrativa deben realizarse de manera obligatoria a través del Sistema Integrado de Compras Públicas (SICOP). Esta centralización busca una gestión más ágil y transparente en la adquisición de bienes y servicios tecnológicos, facilitando, además, el control y la auditoría de las compras públicas.

En este contexto, se fomenta el uso de los convenios marco disponibles en el SICOP, los cuales ofrecen opciones estandarizadas para la adquisición de equipos y servicios. Estos convenios marco facilitan un proceso más eficiente y controlado, reduciendo los tiempos de tramitación y garantizando condiciones comerciales competitivas mediante la agregación de demanda institucional.

Convenios marco para equipos informáticos

En materia de adquisición de equipos, el Ministerio de Hacienda tiene la responsabilidad de coordinar la ejecución de un convenio marco para el arrendamiento y compra de equipos informáticos que satisfaga las necesidades de las instituciones del sector público. Este convenio incluye equipos como computadoras de escritorio, computadoras portátiles y fuentes de poder ininterrumpido (UPS, *Uninterruptible Power Supply*).

Las especificaciones técnicas de los equipos incluidos en el convenio marco deben ser aprobadas por el MICITT, garantizando que los equipos adquiridos cumplan con los estándares técnicos requeridos para el correcto funcionamiento de las entidades públicas. Esta validación técnica busca asegurar la calidad, compatibilidad e interoperabilidad de los equipos con la infraestructura tecnológica existente.

Obligatoriedad y responsabilidades

La implementación de esta Directriz es de cumplimiento obligatorio para todos los jerarcas institucionales y titulares de las entidades públicas, quienes tienen la responsabilidad de velar por su correcta aplicación. Además, se les exhorta a fomentar la participación de otros órganos y entes del sector público en la observancia y ejecución de las disposiciones contempladas en la normativa.

Implicaciones para la gestión tecnológica pública

Esta Directriz transforma la adquisición y el desarrollo tecnológico en un proceso reglado y comparable entre instituciones. Establece un lenguaje técnico común para todo el Estado, lo que facilita la estandarización de soluciones y la agregación de compras. Asimismo, promueve procesos de adquisición más competitivos y transparentes mediante el uso obligatorio del SICOP y los convenios marco.

La estandarización de especificaciones técnicas bajo la validación del MICITT busca garantizar que los equipos y sistemas adquiridos sumen valor público al responder a estándares comunes y a necesidades reales de gestión institucional. Esta aproximación reduce la fragmentación tecnológica, facilita el soporte técnico y el mantenimiento, y potencialmente genera economías de escala en las adquisiciones públicas.

Sin embargo, la efectividad de esta Directriz enfrenta desafíos prácticos. En primer lugar, la obligatoriedad del uso de convenios marco puede presentar inflexibilidades cuando instituciones con necesidades tecnológicas especializadas requieren equipos o configuraciones no contempladas en los catálogos estandarizados. El equilibrio entre estandarización y flexibilidad constituye un reto permanente en la gestión de adquisiciones tecnológicas.

En segundo lugar, la coordinación entre el Ministerio de Hacienda y el MICITT para mantener actualizados los convenios marco requiere procesos ágiles de actualización que sigan el ritmo de evolución tecnológica. Un convenio marco desactualizado puede obligar a las instituciones a adquirir tecnología obsoleta o a recurrir a procedimientos excepcionales que anulan los beneficios de la estandarización.

Finalmente, la supervisión del cumplimiento de las especificaciones técnicas aprobadas por el MICITT exige capacidades de verificación en las instituciones compradoras. Sin personal técnico capacitado que pueda validar que los equipos entregados cumplen efectivamente con las especificaciones contratadas, existe el riesgo de que la calidad técnica se vea comprometida a pesar de la regulación existente.

11. Directriz N.° 133-MP-MICITT (2022) - Mejoras en Ciberseguridad para el Sector Público

La Directriz N.° 133-MP-MICITT (2022) se enmarca en la potestad de dirección del Poder Ejecutivo y reconoce formalmente al Centro de Respuesta a Incidentes de Ciberseguridad de Costa Rica (CSIRT-CR) como instancia coordinadora de la ciberseguridad nacional. Su propósito es elevar, de forma inmediata, las capacidades

técnicas, de atención y de gestión de la ciberseguridad en las instituciones públicas, articulando medidas concretas de prevención, monitoreo y reporte.

Contexto de emisión

Cabe señalar que esta Directriz se origina en el contexto del ataque cibernético masivo contra Costa Rica perpetrado por el grupo cibercriminal Conti en 2022. Los ataques de *ransomware* afectaron múltiples instituciones gubernamentales simultáneamente, evidenciando vulnerabilidades críticas en la postura de ciberseguridad del Estado y la necesidad de una coordinación centralizada de la respuesta. La Directriz constituyó una respuesta institucional inmediata para fortalecer las defensas del sector público.

Obligatoriedad y coordinación técnica

El artículo 1 instruye a la Administración Pública Central, y exhorta a la Descentralizada, a acatar las recomendaciones y medidas técnicas que emita el MICITT por medio de la Dirección de Gobernanza Digital y del CSIRT-CR. La lógica de esta disposición es unificar criterios técnicos y operativos para que las decisiones de seguridad no queden dispersas. Cada institución dispone así de una guía de referencia nacional que orienta sus acciones de protección y respuesta.

Medidas mínimas de resiliencia

El artículo 2 ordena ejecutar de inmediato acciones mínimas de resiliencia de infraestructura, ya sea propia o tercerizada. Estas acciones incluyen la aplicación de actualizaciones de seguridad, el cambio de contraseñas en sistemas institucionales críticos (correo electrónico, sistemas operativos, servidores, redes privadas virtuales o VPN, redes sociales institucionales), la deshabilitación de servicios y puertos innecesarios, y el monitoreo continuo de la red.

La intención de estas medidas es que los eventos adversos sean detectados tempranamente, registrados de forma sistemática y gestionados apropiadamente para limitar su impacto. Estas disposiciones buscan llevar a las instituciones a un estado básico de seguridad que se ha denominado «higiene digital», entendida como el conjunto de prácticas fundamentales que toda organización debe implementar para reducir su superficie de ataque.

Desarrollo de capacidades

El artículo 3 faculta y autoriza la asistencia de los equipos de ciberseguridad y tecnologías de información a las actividades de formación o capacitación que convoquen la Dirección de Gobernanza Digital y el CSIRT-CR. Esta disposición

transforma la construcción de capacidades técnicas de una actividad optativa en un mandato de política pública en donde las instituciones deben facilitar que su personal técnico participe en las capacitaciones organizadas, reconociendo que el factor humano constituye un elemento crítico en la defensa cibernética.

Gestión y reporte de incidentes

El artículo 4 establece el deber de notificar al CSIRT-CR los eventos que afecten la confidencialidad, disponibilidad e integridad de servicios públicos, la continuidad operativa o la suplantación de identidad en redes sociales institucionales. Esta obligación de reporte aplica incluso cuando las instituciones consideren internamente que los incidentes están bajo control.

La Directriz especifica el canal de notificación (*csirt@micitt.go.cr*) y los datos mínimos que debe contener el reporte. Asimismo, exige respaldar la información relacionada con los incidentes para facilitar las investigaciones técnicas y forenses que puedan realizarse posteriormente. Esta centralización del reporte permite al CSIRT-CR mantener una visión consolidada de las amenazas que enfrenta el sector público y coordinar respuestas intersectoriales cuando sea necesario.

Sistema de alertas técnicas

El artículo 6 ordena aplicar las alertas técnicas emitidas por el CSIRT-CR según corresponda a cada entorno institucional. Esta disposición cierra el circuito de inteligencia de amenazas entre alertamiento, remediación y seguimiento a nivel nacional. El CSIRT-CR analiza incidentes, identifica patrones de ataque y vulnerabilidades explotadas, y emite alertas técnicas para que otras instituciones implementen medidas preventivas antes de ser afectadas por las mismas amenazas.

Implicaciones para la gobernanza de ciberseguridad

La Directriz N.° 133-MP-MICITT representa un cambio significativo en la gobernanza de ciberseguridad del sector público costarricense. Al establecer obligaciones concretas y de cumplimiento inmediato, transforma la ciberseguridad de una responsabilidad difusa y voluntaria en un conjunto de deberes formalmente establecidos y supervisados.

La centralización de la coordinación técnica en el CSIRT-CR permite superar la fragmentación que caracterizaba la respuesta institucional previa a los ataques de 2022. El modelo distribuido donde cada institución gestionaba su seguridad de forma aislada demostró ser ineficaz ante amenazas coordinadas y persistentes. La Directriz establece un modelo de coordinación centralizada donde el CSIRT-CR actúa como

punto focal para inteligencia de amenazas, alertamiento temprano y coordinación de respuestas.

Sin embargo, la efectividad de la Directriz enfrenta varios desafíos estructurales. En primer lugar, las medidas mínimas de resiliencia establecidas en el artículo 2 requieren recursos técnicos y humanos que no todas las instituciones poseen de manera inmediata. La aplicación de actualizaciones de seguridad, por ejemplo, puede requerir pruebas previas de compatibilidad que demandan tiempo y personal especializado.

En segundo lugar, la obligación de reporte de incidentes depende de que las instituciones cuenten con capacidades de detección. Una institución sin sistemas de monitoreo o personal capacitado para identificar eventos de seguridad no puede cumplir efectivamente con su deber de notificación. Esto evidencia que las obligaciones de reporte deben acompañarse de inversiones en capacidades de detección.

Finalmente, la sostenibilidad de las capacitaciones mandatorias del artículo 3 requiere que el MICITT y el CSIRT-CR cuenten con recursos permanentes para desarrollar programas de formación a escala. La alta rotación de personal técnico en el sector público, combinada con la evolución constante de amenazas, exige programas de capacitación continua que van más allá de intervenciones puntuales.

12. Acuerdo CONASSIF 5-24 (2024) - Reglamento General de Gobierno y Gestión de la Tecnología de Información

El Acuerdo CONASSIF 5-24 (2024), emitido por el Consejo Nacional de Supervisión del Sistema Financiero (CONASSIF), establece un marco normativo específico para la gestión de la tecnología de información (TI) en las entidades financieras supervisadas en Costa Rica. El CONASSIF, como órgano superior en la estructura de supervisión del sistema financiero nacional, ejerce sus funciones de regulación y supervisión sobre bancos, cooperativas de ahorro y crédito, entidades aseguradoras y otros intermediarios financieros mediante instrumentos normativos como el presente Acuerdo.

Objeto y alcance

El Acuerdo busca garantizar la seguridad de la información y la adecuada gestión de los riesgos tecnológicos en el sector financiero supervisado. Su propósito es minimizar las amenazas cibernéticas y garantizar la continuidad operativa de las entidades en un contexto de creciente digitalización de los servicios financieros, siendo que este marco normativo responde a la necesidad de fortalecer la resiliencia del sistema financiero

frente a riesgos tecnológicos que pueden comprometer no solo la estabilidad de instituciones individuales, sino también la confianza sistémica en el sector.

Gobernanza de la tecnología de información

El Acuerdo subraya la importancia de contar con una estructura organizacional adecuada para la gobernanza de la TI. Establece que los órganos de dirección de las entidades financieras deben asumir la responsabilidad por la supervisión y la toma de decisiones estratégicas relacionadas con los riesgos tecnológicos. Esta disposición sitúa la responsabilidad última sobre la gestión de riesgos tecnológicos en el nivel más alto de la estructura de gobernanza corporativa, reconociendo que las decisiones tecnológicas tienen implicaciones estratégicas para la viabilidad y competitividad de las entidades.

Responsabilidades del órgano de dirección y alta gerencia

El Acuerdo establece que las entidades financieras deben asegurar que tanto el órgano de dirección como la alta gerencia comprendan y asuman sus responsabilidades en la gestión de la TI. Se exige un compromiso explícito con la protección de la privacidad y el secreto de las comunicaciones de los clientes.

La alta gerencia debe implementar políticas efectivas y medidas de control, con especial énfasis en los riesgos asociados a la ciberseguridad. Asimismo, debe poner en práctica medidas preventivas para gestionar los riesgos tecnológicos, asegurando una gestión eficaz y proactiva que identifique vulnerabilidades antes de que sean explotadas y que responda rápidamente cuando ocurran incidentes.

Ciberseguridad y protección de la información

La seguridad de la información constituye uno de los ejes centrales del Acuerdo. Requiere que las entidades implementen mecanismos robustos para gestionar la ciberseguridad, incluyendo actividades como pruebas de vulnerabilidad periódicas, monitoreo constante de sistemas y redes, y procedimientos de respuesta ante incidentes.

Se enfatiza especialmente la protección de la triada de seguridad de la información: confidencialidad, integridad y disponibilidad de los datos. La confidencialidad asegura que la información sensible de clientes y transacciones solo sea accesible a personas autorizadas. La integridad garantiza que los datos no sean alterados de forma no autorizada. La disponibilidad asegura que los servicios financieros permanezcan accesibles para los clientes cuando los requieran.

Servicios en la nube y subcontratación

El Acuerdo regula específicamente el uso de servicios en la nube y la subcontratación de servicios tecnológicos, reconociendo que la externalización de funciones tecnológicas es una práctica cada vez más común en el sector financiero. Establece que los proveedores externos deben cumplir con los estándares de ciberseguridad exigidos a las propias entidades financieras. Además, las entidades deben garantizar que la gestión de la cadena de suministro tecnológica sea segura, protegiendo la infraestructura crítica de posibles vulnerabilidades externas que puedan comprometer la seguridad de la información, esto implica realizar evaluaciones de riesgos de terceros, establecer cláusulas contractuales que garanticen niveles de servicio y seguridad apropiados, y mantener capacidades de supervisión sobre los proveedores contratados.

Auditoría y evaluación continua

El Acuerdo establece que las entidades deben realizar auditorías periódicas internas y externas sobre sus sistemas de TI. Los auditores deben evaluar la efectividad de las políticas y controles implementados, identificando brechas entre los requisitos normativos y las prácticas reales.

Los resultados de estas auditorías deben ser reportados a las autoridades supervisoras pertinentes para su análisis y seguimiento. Esta disposición permite al CONASSIF mantener visibilidad sobre el estado de la gestión tecnológica en el sistema financiero y tomar acciones correctivas cuando sea necesario, ya sea a nivel de instituciones individuales o mediante ajustes al marco regulatorio cuando se identifiquen tendencias sistémicas.

Resiliencia operativa y continuidad del servicio

El Acuerdo enfatiza la importancia de los planes de resiliencia operativa y continuidad del servicio. Estos planes deben incluir estrategias para responder ante incidentes tecnológicos y recuperar la operatividad en casos de desastres, ya sean de origen natural, tecnológico o provocados por actores maliciosos. Además, se requiere que las entidades aseguren la continuidad de los servicios críticos incluso en escenarios de crisis o emergencias. Esto incluye la implementación de sistemas redundantes, procedimientos de respaldo de datos, sitios alternativos de operación y protocolos de comunicación de crisis que permitan mantener informados a clientes, reguladores y otras partes interesadas durante eventos disruptivos.

Implicaciones para el sector financiero supervisado

El Acuerdo CONASSIF 5-24 representa un avance significativo en la regulación del riesgo tecnológico en el sector financiero costarricense. Al establecer requisitos específicos y vinculantes para la gestión de TI, eleva el estándar mínimo de ciberseguridad y resiliencia operativa que deben cumplir las entidades supervisadas. Esta regulación sectorial se complementa con el marco normativo general de ciberseguridad del Estado costarricense, particularmente con la Estrategia Nacional de Ciberseguridad 2023-2027 y el Decreto Ejecutivo N.º 45061-MICITT (2025) sobre gobernanza de ciberseguridad en instituciones gubernamentales. Sin embargo, el Acuerdo CONASSIF reconoce las particularidades del sector financiero, donde la confianza, la protección de activos de clientes y la interconexión sistémica exigen estándares de seguridad especialmente rigurosos.

La efectividad del Acuerdo enfrenta varios desafíos de implementación. En primer lugar, las entidades financieras de menor tamaño, como cooperativas de ahorro y crédito pequeñas, pueden enfrentar dificultades para cumplir con todos los requisitos establecidos debido a limitaciones de recursos técnicos y financieros. La proporcionalidad en la aplicación de los requisitos, considerando el tamaño, complejidad y perfil de riesgo de cada entidad, constituye un desafío regulatorio permanente.

En segundo lugar, la supervisión efectiva del cumplimiento requiere que las superintendencias (SUGEF para bancos, SUGESE para aseguradoras, SUGEVAL para mercados de valores) cuenten con personal técnico especializado capaz de evaluar controles tecnológicos complejos. La brecha de talento en ciberseguridad que afecta al sector privado también impacta a los organismos supervisores.

Finalmente, la evolución acelerada de las amenazas cibernéticas y las tecnologías financieras exige que el marco regulatorio se actualice periódicamente. Un marco normativo que no evolucione al ritmo de la transformación digital puede convertirse en obsoleto o crear barreras inadvertidas a la innovación en servicios financieros digitales.

13. Acuerdo SUGEF 10-07 (2007) - Reglamento sobre Divulgación de Información y Publicidad de Productos y Servicios Financieros

El Acuerdo SUGEF 10-07 (2007), emitido por la Superintendencia General de Entidades Financieras (SUGEF), establece directrices para la divulgación de información y la publicidad de productos y servicios financieros en Costa Rica. Su propósito principal es garantizar la transparencia en las comunicaciones financieras y

proteger a los consumidores mediante la regulación de las prácticas informativas de las entidades supervisadas.

Objeto y ámbito de aplicación

El Acuerdo tiene un enfoque integral orientado a mejorar la claridad de la información proporcionada a los usuarios de servicios financieros y a fortalecer la confianza de los consumidores en los productos disponibles en el mercado. Su ámbito de aplicación abarca todas las entidades financieras bajo supervisión de SUGEF, incluyendo bancos públicos y privados, entidades financieras no bancarias y otros intermediarios financieros autorizados.

Un componente fundamental del Reglamento es la obligación de divulgar información de manera clara, completa y accesible. Las entidades deben mantener actualizada la información sobre sus productos y servicios a través de sus plataformas digitales, particularmente sus sitios web institucionales. Esta información debe incluir características de los productos, tasas de interés, comisiones, cargos aplicables, términos y condiciones, y procedimientos para la atención de consultas y quejas.

La accesibilidad de esta información permite a los consumidores tomar decisiones informadas al comparar productos financieros de diferentes entidades. Asimismo, facilita la supervisión por parte de SUGEF y el ejercicio de controles sociales por parte de organizaciones de defensa del consumidor.

Modificaciones recientes: incorporación de requisitos de ciberseguridad

Mediante modificaciones posteriores al Acuerdo original, se han incorporado requisitos específicos relacionados con la prevención de estafas informáticas y la protección de usuarios en entornos digitales. Estas modificaciones responden al crecimiento acelerado de la banca digital y al aumento de estafas cibernéticas dirigidos a clientes de servicios financieros.

A partir del año 2025, las entidades supervisadas deben implementar controles específicos para mitigar riesgos de fraude informático. El Acuerdo señala la importancia de adoptar medidas de ciberseguridad robustas, tales como la implementación de autenticación de múltiples factores para acceso a servicios en línea, la protección mediante cifrado de información sensible del usuario, y la notificación inmediata a los clientes de cualquier actividad sospechosa detectada en sus cuentas.

Además, las entidades deben ofrecer programas de educación en seguridad digital, asegurándose de que tanto los empleados como los usuarios estén conscientes de los

riesgos informáticos y conozcan las medidas preventivas apropiadas. Estos programas deben abordar temas como reconocimiento de intentos de *phishing*, uso seguro de banca móvil, protección de credenciales de acceso y verificación de la autenticidad de comunicaciones bancarias.

Atención de quejas y reclamos

El Reglamento establece procedimientos que las entidades deben implementar para la atención oportuna y efectiva de quejas y reclamos de clientes. Estos procedimientos deben estar claramente documentados, ser de fácil acceso para los usuarios y garantizar plazos razonables de respuesta.

Sanciones por incumplimiento

El Acuerdo establece que las entidades que no cumplan con las disposiciones sobre divulgación de información, medidas de ciberseguridad y atención de quejas estarán sujetas a sanciones conforme a la Ley N.° 7558, Ley Orgánica del Banco Central de Costa Rica. El régimen sancionatorio puede incluir multas, requerimientos de planes de acción correctiva, restricciones temporales a ciertas actividades, y en casos graves, la revocatoria de licencias de operación.

Implicaciones para la protección del consumidor financiero

El Acuerdo SUGEF 10-07, particularmente en su versión modificada con requisitos de ciberseguridad, representa un instrumento importante para la protección del consumidor financiero en el contexto de la transformación digital del sector. Al integrar obligaciones de transparencia informativa con requisitos de seguridad tecnológica, reconoce que la protección efectiva del consumidor en la era digital requiere tanto acceso a información como protección activa contra amenazas cibernéticas.

La incorporación de requisitos de autenticación multifactor y notificación de actividades sospechosas alinea la regulación costarricense con mejores prácticas internacionales en banca digital segura. Estos controles reducen significativamente la probabilidad de fraudes basados en credenciales comprometidas, que constituyen una de las principales amenazas para usuarios de servicios financieros en línea.

Sin embargo, la efectividad del Acuerdo enfrenta varios desafíos. En primer lugar, la educación de usuarios en seguridad digital requiere esfuerzos sostenidos y creativos. La experiencia internacional muestra que los usuarios frecuentemente ignoran advertencias de seguridad o utilizan contraseñas débiles a pesar de las campañas educativas, por lo que las entidades deben encontrar formas de hacer la

educación en seguridad relevante y accionable para usuarios con diferentes niveles de alfabetización digital.

En segundo lugar, la supervisión del cumplimiento de requisitos de ciberseguridad presenta desafíos técnicos para SUGEF. A diferencia de los requisitos tradicionales de divulgación de información, que pueden verificarse mediante revisión de sitios web y materiales publicitarios, la verificación de la implementación efectiva de controles de autenticación multifactor, cifrado y detección de actividades sospechosas requiere capacidades técnicas especializadas.

Finalmente, la coordinación entre SUGEF y otras instancias regulatorias y de respuesta a incidentes, particularmente el CSIRT-CR, resulta fundamental. Las estafas informáticas contra clientes de servicios financieros frecuentemente son parte de campañas coordinadas que afectan a múltiples entidades simultáneamente. El intercambio de información sobre patrones de ataque y técnicas de fraude permite respuestas más efectivas que las acciones aisladas de entidades individuales.

1.6. Estrategias

1. Estrategia Nacional de Inteligencia Artificial (ENIA) 2024-2027

La Estrategia Nacional de Inteligencia Artificial (ENIA) 2024-2027, publicada por el MICITT en 2024, constituye el instrumento de política pública que ordena el uso, adopción y desarrollo de la inteligencia artificial (IA) en Costa Rica desde una perspectiva ética, segura y responsable. Su objetivo central es maximizar los beneficios sociales de la IA mientras se mitigan los posibles daños a las personas y se protegen los derechos fundamentales.

La Estrategia se construyó mediante un proceso de validación intersectorial que incluyó la participación del sector público, la academia, el sector empresarial y la sociedad civil, reflejando así un enfoque participativo en su formulación.

Enfoque ético y principios rectores

En materia ética, la Estrategia se fundamenta en la Recomendación de la UNESCO sobre Ética de la Inteligencia Artificial y en los Principios de IA de la Organización para la Cooperación y el Desarrollo Económicos (OCDE). A partir de estos marcos internacionales, articula principios rectores centrados en la persona, con énfasis explícito en la paz y la dignidad humana como guías transversales para el diseño, desarrollo y despliegue de sistemas de IA en el país.

Gestión estratégica del riesgo

En materia de gestión de riesgos, la ENIA adopta una visión comparada y pragmática que reconoce diferentes marcos internacionales de referencia. Considera el esquema de clasificación por niveles de riesgo del Reglamento de Inteligencia Artificial de la Unión Europea (*AI Act*), el Marco de Gestión de Riesgos de IA del Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST AI RMF, *AI Risk Management Framework*), y el enfoque evaluativo del Proceso de IA de Hiroshima (HAIP, *Hiroshima AI Process*).

La Estrategia establece que los riesgos deben evaluarse de forma contextualizada antes de implementar sistemas de IA, con especial cuidado en aplicaciones de alto riesgo que puedan afectar ámbitos sensibles como la administración de justicia, la vigilancia y el ejercicio de derechos fundamentales.

Objetivos y prioridades nacionales

La ENIA establece cuatro prioridades estratégicas con sus objetivos asociados:

i. Uso, implementación y desarrollo seguro de la inteligencia artificial.
ii. Transición hacia un nuevo modelo productivo y laboral.
iii. Mejora de servicios públicos y toma de decisiones gubernamentales.
iv. Formación de habilidades y capacidades a lo largo del sistema educativo y de empleo.

Cada prioridad vincula objetivos estratégicos medibles que permiten dar seguimiento a su implementación mediante el plan de acción correspondiente.

Ejes estratégicos de implementación

Operativamente, la ENIA se estructura en siete ejes estratégicos que orientan su implementación:

Eje 1: IA ética, segura y responsable

Este eje tiene por objetivo integrar principios éticos desde el diseño hasta la operación de sistemas de IA, estableciendo mecanismos de validación y certificación del cumplimiento normativo. Incluye el desarrollo de lineamientos de gobernanza de datos que protejan derechos fundamentales, promuevan la inclusión social y garanticen la sostenibilidad de las soluciones implementadas.

Eje 2: Articulación territorial y desarrollo económico

Este eje se orienta a democratizar el acceso a la IA más allá del Gran Área Metropolitana (GAM), mediante la creación de clústeres y laboratorios regionales, el fortalecimiento de redes de colaboración y el apoyo a pequeñas y medianas empresas (PYMES) para modernizar procesos, ganar eficiencia y acceder a nuevos nichos de mercado. Requiere la coordinación entre diferentes niveles de gobierno y el sector privado para asegurar un desarrollo territorial equilibrado.

Eje 3: Promoción de la investigación, desarrollo e innovación

Este eje persigue impulsar la investigación aplicada y la transferencia tecnológica mediante mecanismos de financiamiento, alianzas entre universidades, empresas y el Estado, y el desarrollo de proyectos piloto en sectores estratégicos como agricultura, salud, educación, turismo, manufactura y servicios públicos. El objetivo es generar conocimiento y soluciones de alto impacto adaptadas al contexto nacional.

Eje 4: Gobierno inteligente

Este eje busca la modernización del sector público mediante la incorporación de IA en sus procesos y servicios. Contempla la automatización de trámites, la mejora en la toma de decisiones basada en datos, la personalización de servicios ciudadanos y el fortalecimiento de la transparencia, rendición de cuentas y participación ciudadana. Incluye el desarrollo de capacidades institucionales para la gestión de riesgos e incidentes relacionados con sistemas de IA.

Eje 5: Capacitación y formación de talento

Este eje constituye un elemento fundamental para el desarrollo sostenible de la IA en el país. Propone una agenda nacional de competencias que abarca desde la alfabetización digital hasta programas formales y no formales de formación en IA, desde el nivel de educación primaria hasta posgrado. Incluye programas de actualización profesional, integración del enfoque de género en la formación técnica y el establecimiento de alianzas entre la academia, el sector público y el sector empresarial para construir una base de talento robusta y diversa.

Eje 6: Infraestructura digital y tecnologías habilitantes

Este eje establece los fundamentos técnicos necesarios para escalar el uso de IA en el país. Contempla el desarrollo de conectividad significativa mediante fibra óptica y tecnología 5G, el fortalecimiento de centros de datos y servicios de cómputo en la nube, y la implementación de medidas robustas de ciberseguridad y protección de datos. El objetivo es contar con plataformas tecnológicas resilientes, seguras y evolutivas que soporten aplicaciones avanzadas de inteligencia artificial.

Eje 7: Liderazgo internacional

Este eje final se enfoca en la proyección internacional y la participación en la gobernanza global de la IA. Contempla la participación activa de Costa Rica en foros internacionales como la OCDE, la Alianza Global para la IA (GPAI, *Global Partnership on Artificial Intelligence*), el Proceso de IA de Hiroshima (HAIP) y el Sistema de la Integración Centroamericana (SICA). Busca contribuir al desarrollo de marcos éticos y de interoperabilidad a nivel regional y global, establecer mecanismos de cooperación para cerrar brechas de acceso a la tecnología, y posicionar a Costa Rica como referente en el uso responsable de la inteligencia artificial.

Implicaciones y desafíos de implementación

La ENIA representa un esfuerzo integral por articular una visión estratégica de largo plazo para el desarrollo de la IA en Costa Rica. Su enfoque multidimensional reconoce que el aprovechamiento efectivo de la inteligencia artificial requiere no solo infraestructura tecnológica, sino también marcos éticos sólidos, capacidades humanas desarrolladas, gobernanza apropiada y cooperación intersectorial.

Sin embargo, la efectividad de la Estrategia dependerá de varios factores críticos: la asignación de recursos financieros suficientes para su implementación, el desarrollo de capacidades institucionales para aplicar los marcos de gestión de riesgos propuestos, la articulación efectiva entre los múltiples actores involucrados, y la capacidad del Estado para equilibrar el fomento a la innovación con la protección de derechos fundamentales.

El énfasis en la ética y la seguridad desde el diseño, junto con el reconocimiento explícito de los riesgos asociados a sistemas de IA de alto impacto, refleja una aproximación madura y responsable que busca evitar los efectos adversos observados en otros contextos internacionales donde la adopción de IA ha precedido al desarrollo de marcos regulatorios apropiados.

2. Estrategia Nacional de Ciberseguridad 2023-2027

La Estrategia Nacional de Ciberseguridad 2023-2027 (MICITT, 2023) establece el marco público de referencia para ordenar, desde la perspectiva de derechos y gestión de riesgos, la prevención, mitigación y respuesta frente a amenazas en el entorno digital. Su misión explícita es establecer un marco de acción integral que fortalezca la capacidad de respuesta nacional, promueva una cultura de ciberseguridad y proteja la información personal y crítica del Estado y de la ciudadanía.

Contexto y justificación

La Estrategia parte de un contexto caracterizado por el aumento significativo de ciberataques que han tenido impacto en la seguridad nacional y la economía digital de Costa Rica en años recientes. Los incidentes de 2022, particularmente los ataques de *ransomware* que afectaron múltiples instituciones gubernamentales, evidenciaron la necesidad de replantear el enfoque nacional mediante una estrategia robusta.

Principios rectores y ejes transversales

La Estrategia se fundamenta en cuatro principios rectores: respeto a los derechos humanos y la privacidad, enfoque basado en riesgos y resiliencia cibernética,

coordinación y corresponsabilidad de múltiples partes interesadas, y fomento de la cooperación internacional. Estos principios se articulan mediante cuatro ejes transversales: alianza público-privada, fortalecimiento del marco legal en ciberseguridad y tecnologías de información y comunicación, desarrollo de convenios internacionales, y colaboración y coordinación interinstitucional.

Tabla 6. 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

Pilares estratégicos

La Estrategia se estructura en torno a cinco pilares fundamentales que orientan su implementación:

Pilar 1: Reforzar la gobernanza de ciberseguridad

Este pilar tiene por objetivo implementar un esquema de gobernanza que clarifique funciones, responsabilidades y métodos de interacción entre diversos actores del ecosistema de ciberseguridad. Incluye entidades gubernamentales, el sector privado, instituciones académicas, organizaciones de la sociedad civil y colaboradores internacionales. El enfoque principal es mejorar la coordinación general, fortalecer el liderazgo institucional y optimizar los procesos de toma de decisiones relacionados con la ciberseguridad.

Pilar 2: Adecuar el marco jurídico cibernético

Este pilar se orienta a avanzar en el desarrollo de leyes y regulaciones específicas para el ámbito cibernético, complementadas con normativa técnica enfocada en la ciberseguridad. Busca establecer bases legales y regulatorias sólidas destinadas a promover una gestión eficaz de los riesgos asociados a la ciberseguridad y a

proporcionar las herramientas jurídicas necesarias para contrarrestar las amenazas cibernéticas.

Pilar 3: Fortalecer la protección de infraestructuras y la ciberresiliencia nacional

Este pilar establece la creación de un sistema integral para el manejo de riesgos de ciberseguridad que facilite la identificación, reporte, análisis y respuesta rápida a incidentes. Prioriza el desarrollo de capacidades necesarias para responder a incidentes cibernéticos y promueve una coordinación y comunicación efectiva entre todas las partes involucradas en situaciones de crisis cibernéticas.

Pilar 4: Reforzar las capacidades del ecosistema de ciberseguridad

Este pilar persigue formar una fuerza laboral altamente capacitada en ciberseguridad mediante programas educativos, de entrenamiento y formación profesional. Enfatiza la necesidad de elevar la conciencia sobre ciberseguridad entre la población, fomentando prácticas de comportamiento en línea responsables y seguras. Asimismo, impulsa la investigación y desarrollo en el campo de la ciberseguridad con el objetivo de innovar, mejorar capacidades existentes y mantenerse actualizado frente a las amenazas cibernéticas en constante evolución.

Además, este pilar subraya la importancia del desarrollo del capital humano y la participación ciudadana, incluyendo estrategias para reducir la brecha de género en el sector. Además, promueve el desarrollo de tecnologías, herramientas y metodologías avanzadas para reforzar las capacidades nacionales de defensa en el ámbito de la ciberseguridad.

Pilar 5: Cooperar en el entorno digital

Este pilar final busca promover activamente la cooperación, tanto a nivel nacional como internacional, en materia de ciberseguridad. Incluye la colaboración y el intercambio de información relevante sobre amenazas y mejores prácticas, así como la participación en diversas iniciativas, alianzas y foros internacionales. El objetivo es enfrentar amenazas cibernéticas que trascienden fronteras y contribuir al establecimiento de normativas globales en materia de ciberseguridad.

Visión y misión estratégica

La visión proyectada para 2027 contempla la consolidación de un ecosistema digital confiable que contribuya al esfuerzo global con una fuerza laboral de ciberseguridad desarrollada y competitiva. La misión articula objetivos de prevención, mitigación, innovación y generación de confianza en los sistemas digitales, reconociendo la

interdependencia entre estos elementos para lograr una postura de ciberseguridad robusta y sostenible.

Desafíos de implementación

La implementación efectiva de la Estrategia Nacional de Ciberseguridad enfrenta desafíos significativos. En primer lugar, la sostenibilidad financiera constituye un elemento crítico. La ejecución de los cinco pilares estratégicos exige recursos estables y previsibles que trasciendan el presupuesto anual tradicional, se requiere contar con equipos humanos suficientes, tecnología apropiada para prevenir, detectar, responder y recuperarse ante incidentes, y una planificación de inversiones en horizonte multianual con reglas claras para sostener licencias, servicios gestionados, renovación de infraestructura y ejercicios periódicos de simulación.

Históricamente, Costa Rica ha financiado la ciberseguridad de forma reactiva y fragmentada, principalmente mediante respuestas a crisis puntuales. La transformación de este patrón requiere pasar de proyectos aislados a programas permanentes con indicadores de desempeño y mecanismos de rendición de cuentas. Este cambio implica convertir el gasto de emergencia en capacidad institucional sostenida, un proceso que el MICITT ha venido impulsando mediante la estructuración de la Dirección de Ciberseguridad y sus departamentos especializados.

En segundo lugar, el desarrollo y retención de talento especializado representa otro desafío estructural. La escasez de profesionales en ciberseguridad es un fenómeno global que afecta particularmente al sector público, donde las estructuras salariales y las escalas de carrera profesional dificultan la competencia con el sector privado y las empresas internacionales. La formación de capacidades requiere no solo programas educativos iniciales, sino actualización continua para seguir el ritmo de evolución de amenazas y tecnologías.

En el contexto del sector público costarricense, esto implica diseñar rutas de carrera profesional especializadas, establecer escalas salariales competitivas que desalienten la fuga de profesionales hacia el sector privado, y crear programas de becas, comunidades de práctica y tiempo institucional formal para capacitación. El contexto fiscal del país representa una limitación significativa para implementar mejoras salariales sustanciales, lo que exige explorar mecanismos complementarios como incentivos no monetarios, oportunidades de desarrollo profesional y reconocimiento institucional.

Finalmente, la efectividad de la Estrategia dependerá de la capacidad del Estado para mantener el compromiso político y la continuidad institucional más allá de los ciclos

electorales, asegurando que la ciberseguridad se consolide como política de Estado y no como iniciativa de gobierno.

3. Estrategia de Transformación Digital 2023-2027

La Estrategia de Transformación Digital 2023-2027 (MICITT, 2023) sitúa a la ciudadanía como eje central y entiende la transformación digital como un proceso orientado al servicio público. Su objetivo es desarrollar trámites y servicios digitales, integrados, seguros, interoperables y de alta calidad para mejorar el bienestar ciudadano, cerrar brechas de acceso y modernizar el Estado. El documento se elaboró mediante un proceso colaborativo con participación de instituciones gubernamentales, academia, sector privado y sociedad civil, asumiendo la transformación digital como política pública sostenible y medible en el tiempo.

Contexto y fundamentos

La Estrategia se fundamenta en una trayectoria de gobierno digital que Costa Rica ha venido construyendo desde inicios de la década de 2000, con diversos planes, comisiones y normativas. La actualización estratégica incorpora referentes internacionales de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), la Comisión Económica para América Latina y el Caribe (CEPAL) y los Objetivos de Desarrollo Sostenible (ODS), con el fin de alinear la gobernanza de datos, la transparencia y la interoperabilidad con estándares globales.

Principios rectores y ejes estratégicos

La Estrategia se estructura en torno a seis principios rectores: ética, universalidad, desarrollo humano, creación colaborativa, política pública basada en datos y respeto a la dignidad humana. Estos principios se materializan operativamente mediante dos ejes estratégicos principales: Ciudadanía Digital y Buena Gobernanza.

Eje 1: Ciudadanía Digital

El primer eje prioriza tres componentes fundamentales: identidad y firma digital, servicios y habilidades digitales. La Estrategia establece metas anuales verificables para cada componente. Por ejemplo, el Proyecto de Identidad Ciudadana Digital contempla una programación de implementación del 25 % anual hasta alcanzar el 100 % de cobertura. En materia de servicios digitales, se proyecta la expansión del portafolio disponible en el portal gob.go.cr desde una línea base de 34 servicios hasta 100 servicios, con un incremento de 20 servicios por año.

Tabla 7. 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, 2023-2027.

Estas metas establecen obligaciones concretas para las instituciones en cuanto a la alineación de capacidades institucionales, gestión del cambio organizacional y seguridad desde el diseño *(security & privacy by design*). Este enfoque busca garantizar que la digitalización de servicios incorpore consideraciones de seguridad y privacidad desde las etapas tempranas de planificación y desarrollo.

Eje 2: Buena Gobernanza

El segundo eje incorpora instrumentos habilitadores para la transformación digital. Entre estos destaca el Código Nacional de Tecnologías Digitales (CNTD) como estándar mínimo transversal para proyectos de gobierno digital. El CNTD establece requisitos en materia de accesibilidad, identidad y autenticación, seguridad tecnológica, servicios en la nube, interoperabilidad y neutralidad tecnológica.

En materia de interoperabilidad, la Estrategia define que el modelo para Costa Rica será federado con los datos en la fuente, reduciendo duplicidades y riesgos asociados a la centralización de información. Este eje se vincula con el concepto de Sello de Gobierno Digital, que alinea proyectos públicos a un conjunto de requisitos técnicos y organizacionales verificables antes de su implementación.

Marco de gobernanza: siete pilares estratégicos

La Estrategia se fundamenta en un marco de gobernanza articulado en siete pilares diseñados para orientar el proceso de transformación digital y garantizar su implementación efectiva y sostenible.

Tabla 8. Pilares de la Estrategia de Transformación Digital 2023-2027

Pilar	Casos
1. Personas ciudadanas	**Creación de mecanismos inclusivos que permitan aumentar el acceso a las tecnologías emergentes.**
2. Interoperabilidad	**Interconectividad de los sistemas estatales para el intercambio eficiente de datos.**
3. Ciberseguridad	**Asegurar la protección tanto de la información como de la infraestructura, generando seguridad y confianza.**
4. Marco de políticas	**Alineación estratégica de las políticas públicas para crear un marco integral, coherente y conciso.**
5. Marco jurídico	**Identificación del marco regulatorio que respalda el accionar público en materia digital.**
6. Identidad digital y firma digital certificada	**Herramientas clave para el acceso ciudadano a un gobierno digital.**
7. Digital por diseño	**Simplificación de procesos y generación de canales de comunicación y participación ciudadana.**

Fuente: Elaboración propia con base en la Estrategia de Transformación Digital, 2023-2027.

El Pilar 1 enfatiza la inclusión digital y el acceso universal a tecnologías, reconociendo que la transformación digital debe beneficiar a todos los sectores de la población. El Pilar 2 establece las bases para la integración de sistemas gubernamentales, evitando la fragmentación y facilitando servicios ciudadanos más eficientes.

El Pilar 3 reconoce que la ciberseguridad constituye un elemento transversal sin el cual no es posible generar confianza en los servicios digitales. Los Pilares 4 y 5 abordan la necesidad de actualizar y armonizar el marco normativo y de políticas públicas para habilitar la transformación digital dentro del ordenamiento jurídico vigente.

El Pilar 6 establece la identidad digital y la firma digital certificada como elementos habilitadores fundamentales para la autenticación de ciudadanos en servicios digitales. Finalmente, el Pilar 7 promueve un cambio de paradigma hacia el diseño de servicios digitales por defecto, donde la simplicidad de procesos y la participación ciudadana sean consideraciones primarias desde la concepción de cualquier servicio público.

Implicaciones y desafíos de implementación

La Estrategia de Transformación Digital 2023-2027 representa un avance significativo en la institucionalización de la agenda digital del Estado costarricense. La definición de metas cuantificables anuales permite el seguimiento y la rendición de cuentas sobre el avance de la implementación, además, la incorporación del CNTD como estándar obligatorio busca elevar la calidad técnica de los proyectos de gobierno digital y reducir la heterogeneidad en su implementación.

Sin embargo, la efectividad de la Estrategia enfrenta varios desafíos estructurales. En primer lugar, la transformación digital requiere inversión sostenida en infraestructura tecnológica, desarrollo de capacidades humanas y actualización continua de sistemas. La dependencia de presupuestos anuales puede limitar la capacidad de ejecutar proyectos multianuales con continuidad.

En segundo lugar, la interoperabilidad federada con datos en la fuente requiere que las instituciones cuenten con sistemas de información maduros y estandarizados, lo cual no es uniforme en todo el sector público. La brecha de capacidades institucionales puede generar avances desiguales en la adopción de los estándares establecidos.

Finalmente, la integración efectiva entre la Estrategia de Transformación Digital y la Estrategia Nacional de Ciberseguridad resulta crítica. El objetivo de digitalizar servicios debe equilibrarse con la protección de la información y la gestión de riesgos cibernéticos, lo que exige coordinación estrecha entre las instancias responsables de ambas estrategias y recursos suficientes para implementar controles de seguridad desde el diseño de los servicios digitales.

Investigación y desarrollo de la ciberseguridad

CAPÍTULO III

UNA UNIVERSIDAD NACIONAL COSTA RICA

LABORATORIO DE I+D+i LABCIBE EN CIBERSEGURIDAD

VICERRECTORÍA DE INVESTIGACIÓN UNIVERSIDAD NACIONAL

Para comprender el panorama actual de la ciberseguridad en el país, en el ámbito de la investigación y desarrollo (I+D), conviene mostrar las organizaciones que invierten en este campo y que orientan sus esfuerzos a la generación de conocimiento y a la implementación de soluciones de ciberseguridad. Entre las entidades identificadas se encuentran las siguientes:

2.1 Entidades

2.1.1. Cámara de Tecnologías de Información y Comunicación (CAMTIC)

Organización sin fines de lucro que agrupa a más de 200 empresas y personas profesionales del sector de tecnologías de la información y la comunicación (TIC), incluyendo empresas de ciberseguridad. CAMTIC promueve el desarrollo de acciones consensuadas entre la industria, el Gobierno y la academia (CAMTIC, s. f.).

2.1.2 Cybersec Clúster

Es una agrupación de empresas y organizaciones enfocadas en ciberseguridad, orientada a desarrollar, divulgar y fortalecer el mercado de la ciberseguridad y de tecnologías emergentes en Costa Rica y Latinoamérica. Su propuesta de valor (CyberSec Clúster, s. f.) destaca los siguientes enfoques estratégicos:

- Desarrollo de la industria.
- Desarrollo de talento.
- Desarrollo de mercado.
- Desarrollo de ecosistemas.

2.2. Industria de la ciberseguridad en Costa Rica

A través de la colaboración con CAMTIC, el equipo de LabCIBE-UNA realizó una consulta para identificar las empresas especializadas en ciberseguridad registradas en esta institución. Esta acción forma parte de un esfuerzo más amplio para mapear el ecosistema de ciberseguridad en Costa Rica. A continuación, se presenta la lista de empresas proporcionada por CAMTIC que se dedican específicamente al ámbito de la ciberseguridad en el país. Este listado constituye un insumo para comprender el panorama actual y las capacidades del sector de ciberseguridad costarricense.

- ŠTÍT CYBERSECURITY
- ATTI Cyberlabs
- White Jaguars Cyber Security
- Sofistic
- Grupo B.L
- Grupo Eulen
- SPC Internacional
- AEC Networks
- Sitec Seguridad
- Delta Protect
- CRLabSec
- IMACTUS

Estas empresas, inscritas en CAMTIC y especializadas en ciberseguridad en Costa Rica, ofrecen una amplia gama de servicios destinados a proteger a sus clientes frente a diversas amenazas digitales. Entre los servicios que brindan se incluyen, entre otros:

- **Consultoría en ciberseguridad:** servicios de asesoría para ayudar a las organizaciones a comprender y gestionar sus riesgos de ciberseguridad. Esto puede incluir el diseño de estrategias, la formulación de políticas y la identificación de oportunidades de mejora.
- **Servicios administrados de seguridad (MSSP):** monitoreo y gestión continua de la seguridad de redes, que puede abarcar detección de intrusiones, respuesta a incidentes y administración de controles como *firewalls* y sistemas de detección de intrusiones.
- **Pruebas de penetración y análisis de vulnerabilidades:** evaluación activa de sistemas para identificar y mitigar vulnerabilidades antes de que sean explotadas por actores maliciosos.

- **Cumplimiento normativo y certificaciones:** apoyo para el cumplimiento de estándares, regulaciones y certificaciones aplicables, especialmente relevante en sectores regulados o que administran información sensible.
- **Formación y concienciación en ciberseguridad:** capacitaciones para fortalecer capacidades del personal y reducir la probabilidad de incidentes asociados a error humano.
- **Seguridad de red y *firewalls*:** implementación y gestión de soluciones de seguridad de red, incluyendo *firewalls* de próxima generación (NGFW), para prevenir accesos no autorizados.

2.3. Ciberseguridad en la academia

Con el propósito de comprender el panorama educativo y de investigación en ciberseguridad en el país, resulta pertinente identificar las universidades, tanto públicas como privadas, que desarrollan iniciativas en este ámbito. A continuación, se presenta una lista de universidades que contribuyen al avance de la ciberseguridad mediante programas académicos, proyectos de investigación y colaboración con la industria. Este panorama ofrece una aproximación a los esfuerzos educativos y de desarrollo en el campo.

2.3.1. Sector público

CONARE: El Consejo Nacional de Rectores es una instancia clave del sistema de educación superior pública en Costa Rica. Está integrado por las cinco universidades públicas del país, ampliamente reconocidas por su excelencia académica y por su contribución al desarrollo de la investigación y la educación superior. En este marco, su papel es fundamental para la coordinación y la colaboración interuniversitaria, incluyendo iniciativas vinculadas con áreas críticas como la ciberseguridad (CONARE, s. f.).

Las universidades son:

- Universidad de Costa Rica (UCR)
- Instituto Tecnológico de Costa Rica (TEC)
- Universidad Nacional (UNA)
- Universidad Estatal a Distancia (UNED)
- Universidad Técnica Nacional (UTN)

Dentro de las universidades que conforman CONARE se ofrece una variedad de programas académicos relacionados, de forma directa o indirecta, con el área de la ciberseguridad. Estos programas buscan proporcionar una formación integral y especializada, así como desarrollar competencias para enfrentar los desafíos del campo.

Instituto Tecnológico de Costa Rica (TEC)

Para el año 2025, el Instituto Tecnológico de Costa Rica mantiene activa su Maestría en Ciberseguridad, la cual continúa estructurada en tres énfasis enfocados en seguridad del *software*, defensa y ataque de sistemas, y gestión de la seguridad de la información. Además, el TEC conserva su oferta del programa Técnico en Ciberseguridad Empresarial, diseñado para proporcionar a los estudiantes una

base sólida en la protección de sistemas e información corporativa, dirigido tanto a profesionales como a público general con formación secundaria. (TEC, 2025).

Universidad de Costa Rica (UCR)

Para el año 2025, la Universidad de Costa Rica no cuenta con un programa específico formal en Ciberseguridad, sin embargo, su oferta académica en Ciencias de la Computación e Informática Empresarial continúa incluyendo cursos relacionados con seguridad de la información, redes, sistemas y tecnologías asociadas, los cuales aportan conocimientos parcialmente vinculados al área de ciberseguridad. (UCR, s.f.).

Universidad Nacional (UNA)

Para el año 2025, la Universidad Nacional formalizó la apertura de la Maestría Profesional en Ciberseguridad Industrial en la Sede Regional Chorotega, programa impulsado por el equipo de investigación, desarrollo e innovación LabCIBE, orientado a la protección de infraestructuras críticas, sistemas de control industrial y entornos tecnológicos de alta sensibilidad. (CRHoy, 2025).

Universidad Técnica Nacional (UTN)

Para el año 2025, la Universidad Técnica Nacional no dispone de un programa formal de grado o posgrado especializado en ciberseguridad; no obstante, su carrera de Ingeniería en Tecnologías de la Información continúa incorporando algunos cursos relacionados con redes, seguridad informática y sistemas, los cuales ofrecen una aproximación general a esta área. (UTN, s.f.).

Universidad Estatal a Distancia (UNED)

Para el año 2025, la Universidad Estatal a Distancia no presenta un programa específico dedicado exclusivamente a la ciberseguridad, aunque su carrera de Ingeniería Informática mantiene cursos vinculados a redes, sistemas, bases de datos y seguridad general, los cuales aportan conocimientos complementarios al campo. (UNED, s.f.).

2.3.2. Sector Privado

CONESUP: El Consejo Nacional de Enseñanza Superior Universitaria Privada regula y supervisa las universidades privadas del país. A la fecha de elaboración de este informe, registra 54 universidades privadas. Entre estas, varias destacan por ofrecer carreras, programas técnicos y especializaciones en el campo de la ciberseguridad, lo cual refleja el reconocimiento de la creciente relevancia de esta disciplina en el ámbito tecnológico y empresarial (CONESUP, s. f.).

Universidad Cenfotec

Cenfotec ofrece una Maestría en Ciberseguridad establecida en 2014 y un Técnico en Ciberseguridad. De acuerdo con su sitio web: «El programa de la Maestría en Ciberseguridad de la Universidad Cenfotec ofrece una preparación especializada y una base sólida en la seguridad de las tecnologías de información y comunicación, en un programa que combina experiencia, conocimiento, educación y ética. Está dirigido a profesionales informáticos o de áreas afines, que buscan desarrollarse profesionalmente como administrador de la seguridad de la información, auditor, consultor, investigador, diseñador e implantador de sistemas de seguridad, analista de riesgos de seguridad o probador (*tester*) de la seguridad de sistemas, entre otros». (Universidad Cenfotec, s.f.)

Universidad Latina de Costa Rica

«La Licenciatura en Seguridad Informática de la Universidad Latina de Costa Rica desarrolla conocimientos en cuanto a vulnerabilidades informáticas, intrusión de códigos maliciosos en redes y comunicaciones móviles, desde un marco ético y legal, que permiten la identificación de brechas de seguridad, para el análisis de riesgo que conlleve decisiones estratégicas ligadas a la continuidad del negocio». (Universidad Latina de Costa Rica, s.f.)

Universae

Licenciatura en Ingeniería en Ciberseguridad. «El graduado en este campo es un experto en la gestión segura y eficiente de sistemas informáticos, en arquitectura de seguridad, en tecnología de redes protegidas, y en la integración de medidas de seguridad en equipos electrónicos y sistemas informáticos. Estas habilidades le capacitan para trabajar en una amplia gama de entornos empresariales y tecnológicos, centrando su enfoque principalmente en áreas relacionadas con la ciberseguridad». (Universae, s.f.)

Universidad Fidélitas

Para el año 2025, la Universidad Fidélitas mantiene vigente su oferta de formación en Ciberseguridad mediante el Bachillerato en Ingeniería en Seguridad Informática (Ciberseguridad) y el Técnico Especializado en Ciberseguridad, programas orientados a la formación profesional en protección de sistemas, redes, información y respuesta ante incidentes de seguridad. (Universidad Fidélitas, s.f.).

Lead University

Para el año 2025, Lead University continúa ofreciendo un programa de Técnico Especializado en Ciberseguridad, dirigido a la formación práctica de profesionales

en el área de protección de sistemas de información, redes, análisis de riesgos y seguridad digital. (Lead University, s.f.).

Universidad La Salle

Para el año 2025, la Universidad La Salle mantiene vigente su programa de Técnico en Ciberseguridad, orientado a la formación de talento humano capacitado para proteger sistemas informáticos, redes y activos digitales ante amenazas cibernéticas. (Universidad La Salle, s.f.).

Universidad Castro Carazo

El Técnico en Ciberseguridad 2.0 es un programa virtual de un año de duración, dividido en tres módulos cuatrimestrales, que prepara a los estudiantes para proteger sistemas de información, mantener la integridad de redes y responder a incidentes de seguridad. Ofrece formación integral en áreas como análisis de vulnerabilidades, monitorización de la seguridad de red, configuración de equipos, soporte de nivel 1 y administración de sistemas de seguridad. Además, brinda la oportunidad de optar por insignias digitales (Analista Junior en Ciberseguridad y Técnico en Redes) y prepara para las certificaciones Cisco Certified Support Technician Networking y Cybersecurity (no incluidas en el programa). Inicia el 20 de enero de 2025 y está dirigido a personas con al menos III Ciclo de Educación General Básica, estudiantes de otros programas o profesionales de cualquier disciplina, que cuenten con requisitos técnicos mínimos y dominio básico de lectura en inglés. (Universidad Castro Carazo, s.f.)

Universidad Latinoamericana de Ciencia y Tecnología (ULACIT)

Para el año 2025, la Universidad Latinoamericana de Ciencia y Tecnología (ULACIT) ofrece el Bachillerato en Ciberseguridad bajo modalidad virtual, orientado a la formación de profesionales con competencias en protección de sistemas, redes, análisis de vulnerabilidades, gestión de incidentes y arquitectura de seguridad digital, respondiendo a la demanda creciente de especialistas en el área de la seguridad informática. (ULACIT, s.f.).

Universidad Empresarial de Costa Rica

Para el año 2025, la Universidad Empresarial de Costa Rica incorpora dentro de su oferta académica el programa de Técnico en Ciberseguridad, orientado a la formación práctica de talento humano en protección de infraestructuras tecnológicas, análisis de riesgos, prevención de ataques y respuesta ante incidentes de seguridad digital. (Universidad Empresarial de Costa Rica, s.f.).

Colegio Universitario Boston

Para el año 2025, el Colegio Universitario Boston ofrece el programa de Técnico en Ciberseguridad en modalidad virtual, orientado a la capacitación de estudiantes en protección de redes, sistemas operativos, monitoreo de amenazas, análisis de vulnerabilidades y aplicación de buenas prácticas de seguridad informática para entornos organizacionales. (Colegio Universitario Boston, s.f.).

Universidad Internacional San Isidro Labrador (UISIL)

Para el año 2025, la Universidad Internacional San Isidro Labrador (UISIL) ofrece la Maestría Profesional en Ciberseguridad, programa orientado a la formación de especialistas en gestión de la seguridad de la información, protección de infraestructuras críticas, análisis forense digital, gestión de riesgos tecnológicos y diseño de estrategias de defensa ante amenazas cibernéticas. (Universidad Internacional San Isidro Labrador, s.f.).

Universidad San Marcos

Para el año 2025, la Universidad San Marcos ofrece la Licenciatura en Ingeniería en Sistemas Informáticos con énfasis en Seguridad de la Información, así como un programa técnico de especialización en Ciberseguridad, orientados a la formación de profesionales en seguridad de redes, ciberdefensa, protección de datos, seguridad de aplicaciones y gestión de incidentes en entornos tecnológicos. (Universidad San Marcos, s.f.).

Ministerio de Educación Pública de Costa Rica

El MEP con el aval de CONESUP, ha estado ofreciendo un programa de Técnico en Ciberseguridad desde el año 2020. (Ministerio de Educación Pública de Costa Rica, 2020).

Es evidente que las universidades privadas, a través de estos programas, contribuyen significativamente a la formación de profesionales capacitados y especializados, capaces de afrontar los desafíos de seguridad digital en diversos sectores.

2.3.3. Relevancia de la formación en ciberseguridad para la innovación y la seguridad nacional

El panorama de la educación superior en ciberseguridad en Costa Rica evidencia, para el año 2025, una expansión sostenida tanto en universidades públicas como privadas, reflejando una respuesta progresiva a las crecientes demandas nacionales e internacionales en materia de protección de la información, infraestructuras críticas y entornos digitales.

Desde la perspectiva de la investigación y desarrollo (I+D), la incorporación de programas de posgrado especializados, en particular mencionar a ciberseguridad industrial, seguridad de la información y protección de infraestructuras críticas, incrementa la capacidad nacional para generar conocimiento aplicado, desarrollar soluciones tecnológicas, formar investigadores y establecer vínculos efectivos entre la academia, el sector productivo y el Estado. Asimismo, la amplia oferta técnica y de grado en universidades privadas favorece la creación de una base profesional amplia que alimenta los procesos de investigación, transferencia tecnológica, emprendimiento y fortalecimiento del ecosistema de ciberseguridad en Costa Rica. En conjunto, este escenario posiciona al país en una trayectoria de crecimiento estratégico en el ámbito de la seguridad digital, con alto potencial de impacto en la resiliencia tecnológica, la competitividad económica y la soberanía digital.

2.4 Investigación y Desarrollo

2.4.1. Inversión en I+D en Ciberseguridad

Para el período 2023–2025, el comportamiento de la inversión en Investigación y Desarrollo (I+D) en Costa Rica mantiene una tendencia de estabilidad porcentual respecto al Producto Interno Bruto, sin incrementos estructurales relevantes. Según el *Análisis de los Desafíos del Sector Ciencia, Tecnología, Innovación y Telecomunicaciones*, «la inversión en I+D se ha mantenido constante en 0.34 % como porcentaje del PIB» en el período 2020 a 2022, mientras que la inversión en Actividades Científicas y Tecnológicas ha mostrado una leve disminución (Ministerio de Planificación Nacional y Política Económica (MIDEPLAN, 2024, p. 8). Incluso en la actualización más reciente encontrada a la fecha en (SINCYT, s. f.) es un 0.34 % y sigue constante. No se encontraron actualizaciones más recientes a la fecha.

El documento (MIDEPLAN, 2024, p. 8) también advierte que «al analizar la inversión de los países de la OCDE en I+D, este es del 2,67 %, lo que evidencia los retos país», lo que confirma que Costa Rica continúa muy por debajo de los estándares internacionales en materia de innovación científica. Asimismo, se señala que el sector académico sigue siendo el principal impulsor de la inversión, mientras que la participación del sector público y privado permanece limitada en términos relativos (MIDEPLAN, 2024, pp. 8–9).

2.4.2. Repositorios públicos

Sistema de Bibliotecas, Documentación e Información (SIBDI-UCR) de la Universidad de Costa Rica (UCR). Su sistema de repositorios institucionales incluye acceso abierto a tesis, artículos, publicaciones, proyectos de investigación, etc.; puedes revisar allí para trabajos en informática, seguridad, redes, etc.

- (Repositorio UCR, s.f.) *https://sibdi.ucr.ac.cr/repositorios.php?TR=1*

En Costa Rica, la investigación en ciberseguridad puede ser rastreada a través de repositorios institucionales de universidades públicas y privadas. Por ejemplo, la Universidad Nacional (UNA) mantiene su Repositorio Académico (SIDUNA / RAI).

- (Repositorio UNA, s.f.): *https://www.siduna.una.ac.cr/index.php*

El repositorio del Instituto Tecnológico de Costa Rica (TEC) continúa reuniendo trabajos de graduación, investigaciones y documentos académicos hasta 2025, lo que permite buscar contribuciones con enfoque en seguridad informática.

- (Repositorio TEC, s.f.): *https://repositoriotec.tec.ac.cr*

La Universidad Cenfotec y la Universidad Latina mantienen repositorios activos con múltiples trabajos de graduación recientes en temas de seguridad de la información.

- (Repositorio Cenfotec, s.f.): *https://ucenfotec.librarika.com/search*
- (Repositorio Universidad Latina, s.f.): *https://repositorio.ulatina.ac.cr*

2.4.3. Investigación reciente en ciberseguridad a partir de repositorios académicos en Costa Rica

Los repositorios institucionales de universidades costarricenses son las principales fuentes de investigación y producción académica en el campo de la ciberseguridad, principalmente a través de trabajos finales de graduación, investigaciones aplicadas e informes técnicos. Estos trabajos reflejan un fuerte enfoque aplicado, directamente vinculado con problemáticas reales del sector productivo nacional, lo que fortalece la transferencia tecnológica y la pertinencia de la formación profesional en ciberseguridad. A continuación algunos de las últimas investigaciones encontradas en referencia a Ciberseguridad.

El Instituto Tecnológico de Costa Rica (TEC) continúa aportando investigaciones relacionadas con la integración de la ciberseguridad en contextos empresariales y tecnológicos emergentes. Un ejemplo de ello es el análisis sobre la convergencia entre automatización, ciencia de datos y ciberseguridad como estrategia empresarial, el cual evidencia la creciente interdependencia entre los procesos de transformación digital y la necesidad de mecanismos de protección avanzados en los entornos organizacionales (Instituto Tecnológico de Costa Rica, 2022).

Asimismo, la Universidad de Costa Rica ha generado aportes desde el nivel de posgrado, como el desarrollo de modelos para la detección de URLs maliciosas en tiempo real, lo cual constituye una contribución directa a los sistemas de protección de redes y al combate del cibercrimen desde una perspectiva técnica y experimental (Universidad de Costa Rica, 2024).

De forma complementaria, la Universidad Nacional, por medio del Laboratorio de Ciberseguridad (LabCIBE), publicó en 2025 el informe *Estado de la Ciberseguridad en Costa Rica 2024*, el cual representa uno de los esfuerzos más importantes de sistematización del estado actual del ecosistema nacional en esta materia. El

presente estudio analiza la madurez institucional, los actores involucrados, las brechas estructurales, los desafíos operativos y las oportunidades de desarrollo en el ámbito de la ciberseguridad, consolidando un referente para la formulación de políticas públicas, estrategias académicas y planes de inversión en I+D en seguridad digital (LabCIBE-UNA, 2025).

En el caso de la Universidad Cenfotec, se identifican múltiples proyectos entre los años 2023 y 2024 orientados a la evaluación de sistemas de gestión de ciberseguridad, diseño de soluciones para el intercambio seguro de información y mejora de plataformas empresariales críticas, por poner en ejemplo, algunos temas como la gestión de certificados digitales y la resiliencia de proveedores de servicios de internet. Estos trabajos reflejan un fuerte enfoque aplicado, directamente vinculado con problemáticas reales del sector productivo nacional, lo que fortalece la transferencia tecnológica y la pertinencia de la formación profesional en ciberseguridad (Artavia León & Soto Sotelo, 2023; Universidad Cenfotec, 2024).

En conjunto, la investigación en ciberseguridad desarrollada en Costa Rica, a partir de los distintos repositorios institucionales públicos y privados, presenta una orientación clara hacia la aplicación práctica, la protección de infraestructuras tecnológicas y el fortalecimiento de las capacidades nacionales. No obstante, el proceso de recuperación de información enfrenta ciertos desafíos, ya que no todos los repositorios emplean de manera consistente palabras clave específicas como «ciberseguridad», «seguridad informática» o «ciberdefensa», lo que obliga a utilizar estrategias de búsqueda más amplias basadas en términos como «seguridad», «redes», «informática», «TIC» o «privacidad», así como a realizar revisiones manuales de los contenidos. Adicionalmente, algunos repositorios solo ponen a disposición metadatos básicos como título, autor y resumen, sin acceso al texto completo, lo que requiere la intermediación de bibliotecas o el contacto directo con los autores para obtener los documentos. Finalmente, debido a que una parte importante de esta producción científica mantiene un enfoque aplicado y local, su visibilidad en bases de datos internacionales es limitada, por lo que los repositorios institucionales nacionales continúan siendo la principal fuente primaria para el análisis del avance de la ciberseguridad en el contexto costarricense.

2.4.4. Desafíos en la creación de carreras en Ciberseguridad

El documento Sesión 852-19, 874-20 y 906-21 de CONESUP describe el procedimiento, paso a paso sobre cómo presentar los requisitos para cada tipo de carrera presencial y virtual, los requisitos se resumen brevemente a continuación. (CONESUP, 2021):

1. **Investigación y Justificación:** La institución debe ser capaz de justificar la necesidad y relevancia de la nueva carrera. Esto implica la realización de estudios de mercado,

identificación de brechas en la educación para determinar el nombre y grado de la carrera. Se deben aportar las metas de la carrera, objetivos generales y específicos, la proyección de oportunidades laborales y el perfil profesional de los graduados.

2. **Desarrollo Curricular:** La creación de un plan de estudios sólido y coherente que incluya la descripción estructural de los cursos por ciclo lectivo, programas de los cursos, créditos por curso, horas estudiantes, horas clase, metodología, entre otros detalles relevantes.
3. **Nómina Docente:** Identificar, reclutar y verificar las credenciales de un equipo docente adecuado puede ser un desafío, especialmente si se buscan profesionales con experiencia y especialización en áreas recientes o de vanguardia. En esta parte se deben presentar *curriculum vitae* de los docentes propuestos, grado académico y experiencia de estos, entre otras cosas.
4. **Requisitos académicos:** Estos son los requisitos que el estudiante debe contar para el ingreso así como los requisitos de graduación. Así como presentar los títulos que se otorgaran al completar la carrera.
5. **Análisis comparativo:** Debe presentarse una comparación de la propuesta curricular con respecto a otras universidad estatales o internacionales.
6. **Director de carrera:** Presenta carta debidamente firmada por la persona propuesta como director de carrera en la que consigne expresamente la aceptación al respectivo cargo por un plazo mínimo de un año.
7. **Infraestructura:** La institución debe contar con las instalaciones adecuadas, laboratorios, recursos bibliográficos y tecnológicos para soportar la enseñanza y el aprendizaje de calidad.
8. **Regulaciones y cumplimiento:** Presentar el certificado del permiso de autorización emitido por la Dirección de Equipamiento e Infraestructura (MEP), donde se especifique la oferta académica autorizada, la nueva carrera a impartir y capacidad locativa. Asimismo, permiso sanitario de funcionamiento del Ministerio de Salud, certificado de aprobación del Consejo de Salud Ocupacional, registro de propiedad de las instalaciones físicas, o bien, la copia auténtica del contrato de arrendamiento firmado por el representante legal. Finalmente, el certificado de la patente municipal correspondiente. Son una serie de permisos y autorizaciones que se deben obtener de diferentes entidades. Cada uno de estos pasos puede tener sus propios requisitos y tiempos de espera.
9. **Aspectos Financieros:** Establecer tarifas, presenta las tarifas para ser aprobadas por el órgano competente de conformidad con la nueva metodología.

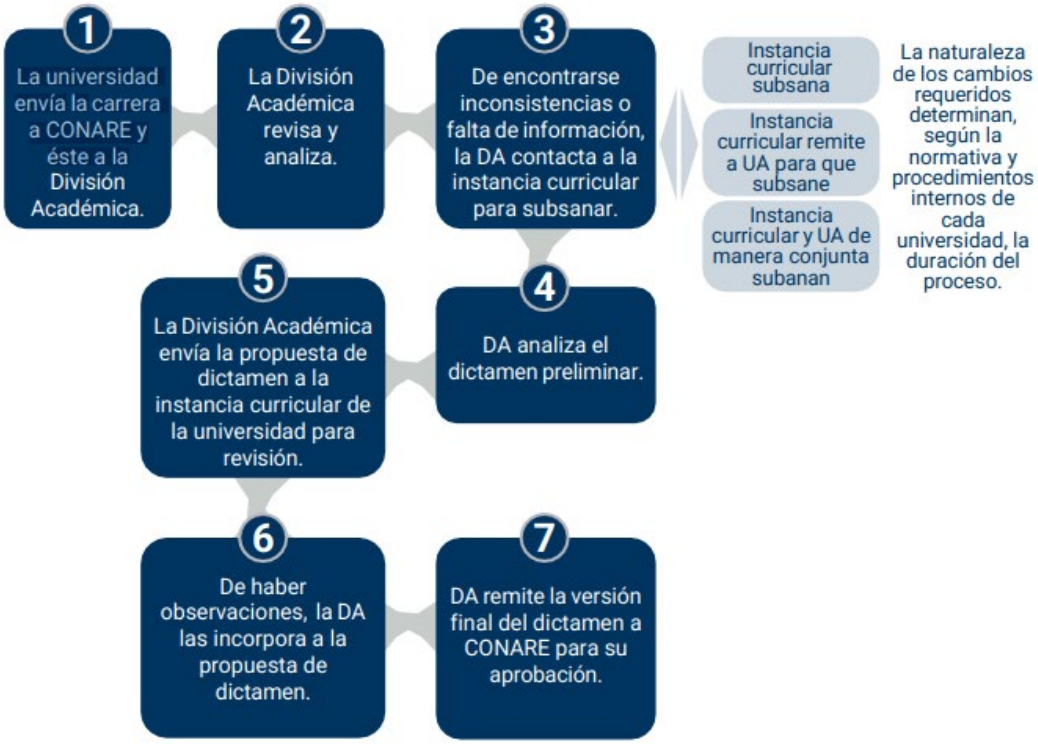
El proceso de apertura de una carrera virtual tiene requisitos compartidos con el proceso presencial, y además, incluye:

1. **Solicitud Modalidad Virtual:** Es necesario presentar varios contratos, incluidos aquellos relacionados con el soporte técnico, licencias de *software*, bibliografía y otras bases de datos bibliográficas.

2. **Modelos pedagógicos virtuales:** La universidad debe presentar el modelo pedagógico que guiará la carrera.
3. **Requisitos básicos Administración Virtual:** Deben describirse varios aspectos, como la infraestructura, la plataforma tecnológica, la estructura de apoyo administrativo, y los procedimientos relacionados con la comunicación.

En cuanto al proceso establecido por el CONARE, este constituye un proceso similar, en términos de complejidad y duración. No obstante, el documento Proceso General de Aprobación de Carreras de CONARE cuenta con diferentes lineamientos para la creación y el rediseño de carreras Universitarias estatales, el cual consiste en 7 etapas cuya duración es determinada por la naturaleza de los cambios requeridos y puede cambiar según la normativa y procedimientos internos de cada universidad.

Figura 1. Proceso General de Aprobación de Carreras

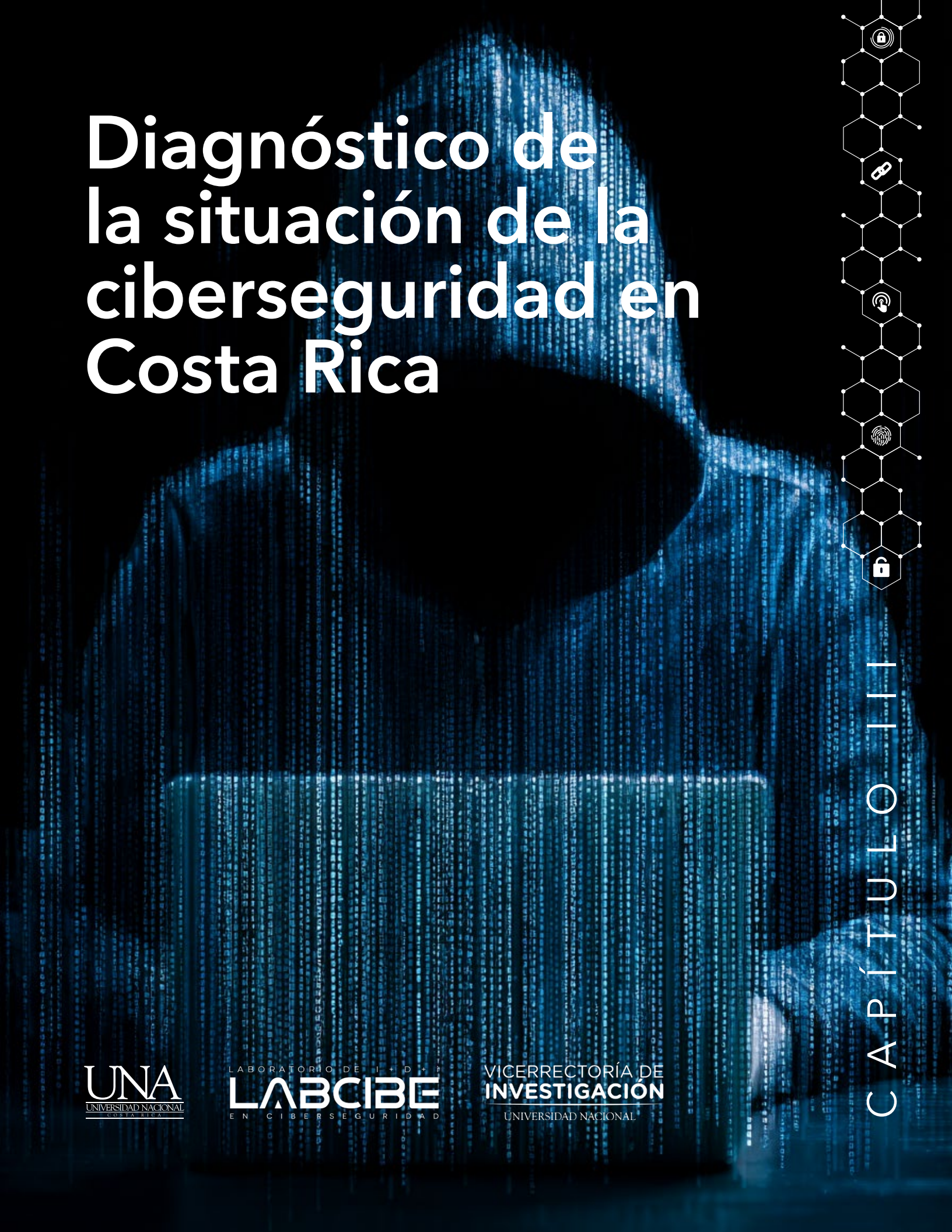


Fuente: Comisión de Currículo Universitario, 2022

La creación y modificación de carreras universitarias, especialmente en un campo tan dinámico como la ciberseguridad, es un proceso complejo y prolongado, que generalmente puede durar años. Ajustar estos programas no es una tarea sencilla; involucra múltiples etapas que incluyen investigación y justificación exhaustivas, desarrollo curricular detallado, reclutamiento de un equipo docente especializado, y la obtención de numerosas autorizaciones y cumplimientos regulatorios.

Estos procesos, tanto en universidades privadas reguladas por CONESUP como en universidades públicas bajo CONARE, son rigurosos y requieren tiempo para garantizar que los programas sean relevantes, de alta calidad y alineados con las necesidades actuales y futuras del campo profesional. Por lo tanto, aunque la adaptación es necesaria para mantenerse al día con los avances tecnológicos, las instituciones enfrentan desafíos significativos debido a la naturaleza prolongada y compleja de estos procesos de modificación y aprobación.

Diagnóstico de la situación de la ciberseguridad en Costa Rica



CAPÍTULO III

UNA UNIVERSIDAD NACIONAL COSTA RICA

LABORATORIO DE I+D+i LABCIBE EN CIBERSEGURIDAD

VICERRECTORÍA DE INVESTIGACIÓN UNIVERSIDAD NACIONAL

Esta sección presenta un análisis detallado de los resultados obtenidos a través de la encuesta aplicada en el marco de la investigación sobre el estado de la ciberseguridad nacional, con énfasis en los componentes de investigación y desarrollo, así como en la dimensión jurídica de la ciberseguridad en Costa Rica.

El objetivo principal del estudio es determinar, de forma anual, el estado de la ciberseguridad en Costa Rica desde una perspectiva técnica, normativa y de gestión. Para ello, se recurre a consultas clave que permiten caracterizar, de manera estadística, la situación nacional y formular conclusiones de alcance general (no particular por institución). Este enfoque busca identificar desafíos actuales y proponer recomendaciones orientadas a fortalecer el entorno de ciberseguridad del país.

3.1. Diseño de la Encuesta sobre el estado del arte en la Ciberseguridad

El Laboratorio de Investigación, Desarrollo e Innovación en Ciberseguridad (LabCIBE) de la Universidad Nacional desarrolla esta encuesta con el propósito de diagnosticar el estado de la ciberseguridad en Costa Rica desde una perspectiva integral, que abarca aspectos jurídicos, operativos, técnicos y de investigación orientada al desarrollo. El instrumento incorpora temas como gobernanza institucional, gestión y prevención de incidentes, controles de ciberseguridad, capacitación y protección de datos personales, inteligencia artificial aplicada a la ciberseguridad, así como recursos y presupuesto asignados en esta materia.

Para ello, se diseñó una encuesta dirigida a actores clave vinculados a investigación y desarrollo y con la gestión operativa de la ciberseguridad, incluyendo instituciones del sector educativo, entidades públicas y organizaciones del ámbito productivo. Este enfoque permite obtener una visión amplia y detallada sobre la dimensión regulatoria, el estado jurídico, la capacidad operativa y las capacidades de desarrollo tecnológico en ciberseguridad a nivel nacional.

La encuesta busca identificar tanto la existencia de programas o iniciativas orientadas a fortalecer la investigación y la innovación como la percepción institucional respecto del marco normativo vigente y del nivel de preparación organizacional frente a las amenazas cibernéticas. El presente informe fue sometido a un proceso de revisión técnica y editorial para garantizar la consistencia interna entre tablas, gráficos, fuentes y texto analítico.

3.1.1. Encuesta 2025

A continuación, se presenta el instrumento de encuesta utilizado en la edición 2025 del estudio *Estado de la Ciberseguridad en Costa Rica*. Este cuestionario fue aplicado a diversos actores del ecosistema nacional, instituciones públicas, entidades del sector financiero, empresas privadas, academia y otros organismos clave, con el fin de recabar información homogénea y comparable sobre su situación en materia de ciberseguridad, gestión de riesgos, protección de datos e innovación tecnológica. La inclusión del instrumento en este informe busca reforzar la transparencia metodológica, facilitar la replicabilidad del estudio en futuras ediciones y permitir a las personas lectoras comprender el alcance y los enfoques analíticos que sustentan los resultados presentados.

Preguntas específicas sobre el estado de I+D

1. ¿La institución ofrece programas de formación o cursos específicos en ciberseguridad (orientados a desarrollo de capacidades técnicas y/o I+D)?

- ○ Sí, oferta formal y vigente (catálogo estable)
- ○ Sí, ocasional / ad hoc
- ○ En diseño/planificación
- ○ No
- ○ No sabe / No responde

Si su respuesta es «Sí», por favor especifique los programas o cursos ofrecidos.

2. ¿La institución mantiene convenios/alianzas vigentes con otras organizaciones para la formación en ciberseguridad (docencia, capacitación, pasantías o co-desarrollo)?

- ○ Sí, con convenio/contrato vigente
- ○ Sí, pero inactivo/expirado en los últimos 12 meses
- ○ En negociación/planificación
- ○ No
- ○ No sabe / No responde

3. ¿Qué tan efectiva ha sido la implementación de los convenios de formación en ciberseguridad y los resultados obtenidos en los últimos 12 meses?

- ○ Muy efectiva
- ○ Efectiva
- ○ Neutral
- ○ Poco efectiva
- ○ Nada efectiva

4. ¿Su institución cuenta con presupuesto dedicado para actividades de investigación y desarrollo (I+D) en ciberseguridad?

- ○ Sí, con línea presupuestaria específica (anual o plurianual)
- ○ Sí, pero dentro del presupuesto general de I+D/capacitación (sin línea específica)
- ○ En evaluación/planificación
- ○ No
- ○ No sabe / No responde

5. En los últimos 12 meses, ¿su institución ha ejecutado proyectos de investigación en ciberseguridad?

- ○ Sí
- ○ No
- ○ No sabe / No responde

6. En los últimos 12 meses, ¿su institución ha formulado proyectos de investigación en ciberseguridad o tiene intención de formularlos?

- ○ Sí
- ○ No
- ○ No sabe / No responde

7. Si la respuesta anterior es «Sí», por favor especifique:

- ○ Investigación
- ○ Desarrollo
- ○ Ambas

8. ¿En cuál(es) de las siguientes áreas específicas de ciberseguridad se enfocan las investigaciones y desarrollo actuales de su institución? (Seleccione todas las que apliquen)

- ○ Seguridad de redes
- ○ Seguridad en la nube
- ○ Seguridad de aplicaciones y *software*
- ○ Seguridad de Internet de las Cosas (IoT)
- ○ Seguridad de sistemas industriales (ICS/SCADA)
- ○ Análisis y detección de *malware*
- ○ Respuesta a incidentes y gestión de riesgos
- ○ Inteligencia artificial aplicada a la ciberseguridad
- ○ Privacidad y protección de datos

- Seguridad en *blockchain* y criptomonedas
- Concientización y formación en ciberseguridad
- Cumplimiento normativo y legal
- Análisis forense digital
- Otro (por favor especifique).

9. ¿Qué productos tangibles ha generado la investigación + desarrollo en ciberseguridad en su institución en los últimos 12 meses?

- Publicaciones académicas
- Patentes
- Propiedad intelectual
- Prototipos o *software* desarrollado
- Servicios implementados en la industria
- Estándares/guías prácticas
- Otro

10. ¿Cuenta su organización con planes futuros en términos de investigación y desarrollo en ciberseguridad?

- Sí
- No
- No sabe / No responde

11. ¿Cuáles considera los principales desafíos que enfrenta su institución en cuanto a I+D en ciberseguridad?

- Financiamiento
- Escasez de personal calificado
- Acceso a datos/infraestructuras
- Colaboración público-privada/público-público

12. ¿Qué nivel de importancia considera que tiene la investigación y desarrollo en ciberseguridad en su institución?

- Muy Importante
- Importante
- Poco Importante
- No es Importante
- No sabe / No responde

13. ¿En qué medida está de acuerdo con la siguiente afirmación?: «Las actividades de investigación y desarrollo (I+D) en ciberseguridad en las instituciones académicas de Costa Rica se limitan principalmente a los proyectos de fin de carrera de los programas de posgrado».

- ○ Muy de acuerdo
- ○ De acuerdo
- ○ En desacuerdo
- ○ Muy en desacuerdo
- ○ Neutral

14. ¿Desea agregar comentarios, evidencias o recomendaciones sobre el estado actual de la investigación y desarrollo (I+D) en ciberseguridad en su institución?

Preguntas específicas sobre la situación jurídica de la Ciberseguridad Nacional

Ciberseguridad

La presente sección tiene como objetivo identificar el grado de relevancia institucional en torno a ciberseguridad y conocer si las organizaciones han sido víctima de ataques cibernéticos en el último año (2024 - 2025).

1. ¿Qué nivel de preocupación le asigna hoy a cada riesgo/amenaza de ciberseguridad? Considere probabilidad e impacto en su institución.

- ○ *Phishing*/BEC (suplantación de autoridad)
- ○ *Ransomware* y extorsión
- ○ Pérdida o filtración de datos (exfiltración, fuga accidental)
- ○ Vulnerabilidades y parches (CVE/KEV, desactualización)
- ○ Credenciales débiles/comprometidas (*password reuse*, *brute force*)
- ○ Terceros y cadena de suministro (proveedores/SaaS/MSP)
- ○ Nube/misconfiguraciones (M365, Google, AWS, etc.)
- ○ Disponibilidad/DoS (servicios críticos)
- ○ Insider/abuso de privilegios (personal/contratistas)
- ○ *Malware* en *endpoints* (*no ransomware*)
- ○ *Software* no autorizado/piratería (*shadow IT*/licencias)
- ○ OT/IoT/industrial (si aplica)

2. ¿Cuenta con una póliza de ciberseguro vigente para cubrir incidentes de seguridad de la información o ciberseguridad?

- ○ Sí
- ○ En trámite/renovación
- ○ No
- ○ No sabe / No responde

3. ¿Su institución está interesada en contratar una póliza de ciberseguridad?

- ○ Sí
- ○ No

4. ¿En qué plazo tiene pensado adquirir una póliza de ciberseguridad?

- ○ En < 3 meses
- ○ En 3–6 meses
- ○ En 7–12 meses
- ○ Sí, pero sin plazo definido
- ○ En evaluación (estudio de mercado)
- ○ No, por ahora
- ○ No sabe / No responde

5. ¿Ha sufrido alguno de los siguientes ataques en 2025?

- ○ Infección de *ransomware* (robo/secuestro de información))
- ○ Fraude/Estafa
- ○ Robo de información
- ○ Exposición de vulnerabilidades
- ○ Acceso Indebido a bases de datos
- ○ Alteración de sitio web

6. En caso de haber sufrido alguno de estos ataques en sus sistemas de información, ¿procedió a denunciarlo ante el Sistema Judicial?

- ○ Si
- ○ No
- ○ No sabe / No responde

Estado de la ciberseguridad

7. ¿En su institución cuentan con algún protocolo de actuación ante un incidente en sus sistemas de información?

8. ¿En su institución se cuenta con algún reglamento, política, circular o directriz sobre el uso de los equipos de tecnologías de la información?

9. En caso de contar con una Política de Ciberseguridad ¿En cuáles canales se comunica la política de ciberseguridad y las buenas prácticas al personal?

10. ¿En qué medida participa la Alta Dirección (Dirección General/Junta) en la gobernanza de la ciberseguridad?

11. ¿Cuáles de las siguientes fuentes y mecanismos utiliza la institución para mantenerse actualizada sobre las tendencias y amenazas en ciberseguridad?

- ○ Alertas de CSIRT/CERT (nacional o sectorial)
- ○ Boletines de autoridades (p. ej., CISA, ENISA, NCSC)
- ○ Avisos de seguridad de proveedores (Microsoft, Oracle, Cisco, Fortinet, etc.)
- ○ *Feeds*/servicios de *Threat Intelligence* (STIX/TAXII, comerciales o comunitarios)
- ○ Listados de vulnerabilidades (CVE/NVD, catálogos KEV)
- ○ Participación en conferencias / seminarios / *webinars*
- ○ Participación en foros / comunidades profesionales (p. ej., OWASP, capítulos locales)
- ○ Suscripción a bases de datos/revistas especializadas
- ○ Programas de formación/capacitación (LMS, certificaciones)
- ○ Consultoría externa / MSSP (monitoreo, *advisories*)
- ○ Intranet/boletines internos de TI/Seguridad
- ○ Redes sociales oficiales de CERT/autoridades/proveedores
- ○ No sabe / No responde

12. ¿Existen revisiones periódicas del estado de la seguridad de los sistemas de información en su institución?

13. ¿Con qué frecuencia se realizan?

14. De los siguientes controles de ciberseguridad ¿De cuáles dispone la institución?

- ○ MFA (autenticación multifactor)
- ○ SSO / IdP (Azure AD/Entra, Okta, etc.)
- ○ Active Directory local (*on-premises*)
- ○ PAM (gestión de cuentas privilegiadas)

- NAC/802.1X (control de acceso a red)
- *Secure Email Gateway* (*antispam*/anti-*phishing*)
- SPF / DKIM / DMARC configurados
- Filtrado web/Proxy/DNS seguro
- *Sandboxing* de adjuntos/URLs
- EDR/XDR
- Antivirus/*antimalware* tradicional (si no usa EDR)
- MDM/UEM (gestión de móviles/equipos)
- Gestión automatizada de parches
- *Firewall*/NGFW
- IDS/IPS
- NDR (detección en red)
- VPN/SD-WAN/SASE
- WAF (*firewall* de aplicaciones web)
- DLP (prevención de fuga de datos)
- Cifrado en reposo y en tránsito
- Backups con regla 3-2-1 y/o inmutables/*offline*
- CSPM/CIEM/CWPP (seguridad en nube)
- SIEM/SOAR (*logs* centralizados y orquestación)
- Gestión de vulnerabilidades (escáner/KEV)
- *Baseline/hardening* (CIS u otras guías aplicadas)
- No sabe / No responde
- Otros (especifique).

Prevención de incidentes

15. ¿Quién es el responsable primario de la gestión de incidentes de seguridad de la información (prevención, detección, respuesta y recuperación) en su institución?

16. ¿Qué áreas participan operativamente en la prevención y respuesta a incidentes?

17. ¿En su institución se implementa algún mecanismo de evaluación de riesgo cibernético?

18. ¿La institución restringe el acceso a la red corporativa desde dispositivos personales no gestionados?

19. ¿Existe algún instrumento normativo vigente que regule el uso y administración de redes sociales institucionales (p. ej., Facebook, X/Twitter, Instagram, TikTok, YouTube, LinkedIn, WhatsApp/Telegram)?

20. ¿La institución implementa medidas técnicas para cumplir la Ley N.º 8968 y su Reglamento en el tratamiento de datos personales de clientes/usuarios?

21. ¿De dónde considera proviene principalmente el riesgo de ciberseguridad (probabilidad × impacto) en su institución?

22. ¿Cómo gestiona su institución el uso de medios de almacenamiento removible (USB, discos externos, tarjetas SD) en equipos corporativos?

23. ¿La institución realiza simulaciones de *phishing* u otros ejercicios de ingeniería social para evaluar y mejorar la preparación del personal?

24. ¿Qué tan frecuente son este tipo de simulacros?

Programas de capacitación y/o formación

25. ¿Con qué frecuencia la organización participa u organiza eventos como conferencias o talleres sobre ciberseguridad?

26. ¿En cuáles de los siguientes temas ha recibido capacitación o formación el personal de su institución?

- ○ Concienciación en ciberseguridad (uso aceptable, higiene digital)
- ○ *Phishing* e ingeniería social (correo, SMS, *vishing*, QR, BEC)
- ○ Contraseñas seguras y autenticación multifactor (MFA)
- ○ Protección de datos personales y privacidad (Ley N.º 8968)
- ○ Clasificación y manejo de información / DLP / «mesa limpia»
- ○ Seguridad en dispositivos móviles, portátiles y Wi-Fi
- ○ Teletrabajo/Trabajo remoto (VPN, BYOD, nube)
- ○ Redes sociales y huella/identidad digital
- ○ Respuesta a incidentes: reporte y primeros pasos del usuario
- ○ (Técnico) Gestión de incidentes/IR para equipos de TI/Seguridad
- ○ (Técnico) Vulnerabilidades y parches
- ○ (Técnico) Seguridad en nube/SaaS (M365/Google/AWS)
- ○ Cumplimiento legal y delitos informáticos
- ○ Otros (especifique).

27. ¿La capacitación en ciberseguridad es obligatoria para todo el personal de la organización (independientemente del cargo)?

28. ¿La institución dispone de presupuesto para financiar certificaciones profesionales en ciberseguridad (exámenes, renovaciones y/o preparación)?

29. ¿La institución ofrece programas de formación continua en línea (*e-learning*) en ciberseguridad para su personal?

Procedimiento Legal

30. ¿Qué tan familiarizado(a) está con la normativa penal costarricense sobre delitos informáticos (reformas al Código Penal, conocida como «ley de delitos informáticos»)

31. ¿La normativa penal costarricense sobre delitos informáticos (reformas al Código Penal) cubre los incidentes informáticos en el país?

32. ¿Por qué?

33. ¿Considera que las sanciones legales en Costa Rica por delitos informáticos son suficientemente disuasorias como para prevenir incidentes cibernéticos?

Recursos y Presupuesto

34. ¿Qué porcentaje del presupuesto de TI se destina a ciberseguridad?

35. ¿Considera que este presupuesto es adecuado para las necesidades de ciberseguridad de su institución?

36. De la siguiente lista ¿La institución subcontrata algún servicio relacionado con ciberseguridad?

- ○ Monitoreo de seguridad (SOC/SIEM/MDR/XDR)
- ○ Respuesta a incidentes y forense (*retainer*)
- ○ Gestión de vulnerabilidades (escaneo y priorización)
- ○ Pruebas de penetración / *Red Team*
- ○ Auditorías de seguridad / *compliance* (ISO 27001, PCI, etc.)
- ○ Gestión de identidad y acceso (IdP/SSO/MFA)
- ○ Seguridad en nube (CSPM/CIEM/CWPP)
- ○ *Threat intelligence* (*feeds*/IOCs)
- ○ Educación y concienciación (incluye simulaciones de *phishing*)
- ○ Protección de datos y privacidad (DPO externo, DPIA)

37. ¿Su institución desarrolla actividades en mercados internacionales?

38. ¿En qué áreas geográficas a nivel mundial tiene presencia o realiza operaciones la organización?

39. ¿Ha evaluado los riesgos de ciberseguridad específicos para esos mercados?

40. ¿Ha adaptado la organización sus políticas de ciberseguridad según las regulaciones y normativas presentes en los diferentes mercados internacionales en los que opera?

41. ¿La institución utiliza VPN u otras tecnologías para proteger las comunicaciones internas y externas?

42. ¿Ha experimentado la organización algún ataque cibernético en alguna de sus operaciones fuera de Costa Rica?

Inteligencia Artificial

43. ¿La institución utiliza (o está realizando pilotos) capacidades de inteligencia artificial, tradicional o generativa, en procesos de ciberseguridad?

44. De la siguiente lista ¿En qué áreas específicas de ciberseguridad se ha implementado el uso de la inteligencia artificial?

- ○ Administración de accesos
- ○ Detección de amenazas
- ○ Análisis de conductas/comportamiento
- ○ Respuesta automática a incidentes
- ○ Gestión de vulnerabilidades (priorización por riesgo/explotabilidad)
- ○ Investigación de incidentes (resumen de *logs*, *timelines*, reportes con LLM)
- ○ Protección de datos
- ○ SIEM/SOC (correlación, *triage* y priorización de alertas)
- ○ EDR/XDR/MDR (detección/contención en *endpoints*)
- ○ UEBA (análisis de conducta de usuarios/entidades)
- ○ NDR / tráfico de red (anomalías)
- ○ *Anti-phishing*/BEC en correo
- ○ Threat intelligence (enriquecimiento/IOCs)
- ○ Análisis de *malware* (*sandboxing*/clusterización)
- ○ SOAR / respuesta automatizada (*playbooks* asistidos por IA)
- ○ Gestión de identidades y acceso (riesgo adaptativo, anomalías de *login*)
- ○ Clasificación de datos / DLP (etiquetado inteligente, seudonimización)
- ○ DevSecOps (revisión de código, dependencias, IaC)
- ○ Seguridad en nube (CSPM/CIEM/CWPP con ML)
- ○ Fraude / antiabuso (si aplica a su operación)
- ○ Otros (especifique).

45. En términos evaluativos ¿Cómo considera la aplicación de soluciones de IA en su institución?

46. ¿Cuáles son los tres principales desafíos para implementar (o escalar) IA en ciberseguridad en su institución? (Marque hasta 3)

- ○ Integración con herramientas/procesos existentes (SIEM/EDR, *ticketing*, IR)
- ○ Calidad y gobernanza de datos (inventario, etiquetado, acceso)
- ○ Privacidad y cumplimiento (Ley N.° 8968, contratos, transferencias internacionales)
- ○ Seguridad de modelos y datos (exfiltración de *prompts*, ataques adversariales, *shadow AI*)
- ○ Talento y capacidades internas (SOC/analistas, MLOps/IA)
- ○ Presupuesto / costo total de propiedad (licencias, infraestructura, operación)
- ○ Dependencia/*lock-in* de proveedor y *due diligence* de terceros (MSSP/LLM)
- ○ Explicabilidad/confianza de los modelos y riesgo operativo
- ○ Gobernanza y política de uso de IA (roles RACI, revisión humana)
- ○ Infraestructura tecnológica (GPU, latencia, conectividad/nube)
- ○ Gestión del cambio y cultura (resistencia, adopción)
- ○ ROI/beneficio no demostrado
- ○ Otros (especifique).

47. ¿La institución cuenta con personal calificado en inteligencia artificial (IA) aplicable a ciberseguridad?

48. ¿La institución invierte actualmente en formación y capacitación en inteligencia artificial (IA) aplicada a la ciberseguridad?

La estrategia de levantamiento de información se basó en la difusión de la encuesta a organizaciones públicas y privadas vinculadas al sector tecnológico, académico y productivo, así como a entidades públicas que integran espacios formales de coordinación institucional. No se dispone de un marco muestral cerrado que permita identificar con precisión el número total de organizaciones invitadas, por lo que no es posible calcular una tasa de respuesta. En consecuencia, los resultados deben interpretarse como un diagnóstico descriptivo de las organizaciones participantes y no como una estimación probabilística representativa del conjunto del país. Esta limitación se declara de forma explícita para resguardar el rigor metodológico del análisis.

3.1.2. Alcances y limitaciones metodológicas del levantamiento 2025

El levantamiento de información correspondiente a la edición 2025 se realizó mediante una encuesta nacional dirigida a organizaciones del sector público y privado, a través de órganos representativos, cámaras empresariales, asociaciones profesionales, entes reguladores y redes institucionales vinculadas al ámbito tecnológico y de la ciberseguridad.

La estrategia de difusión del instrumento se basó en la circulación de la encuesta a través de dichas organizaciones y redes sectoriales, lo que permitió alcanzar una participación amplia y diversa. No obstante, debido a esta modalidad de distribución, no fue posible establecer con precisión el universo total de entidades receptoras de la invitación, ni calcular una tasa de respuesta formal.

La encuesta registra internamente el nombre de la organización participante con el objetivo de prevenir duplicidades, validar la consistencia de la información y fortalecer la calidad del análisis. Sin embargo, esta información no se publica ni divulga, en cumplimiento de principios de confidencialidad y protección de datos, y dado que el análisis se realiza exclusivamente de forma agregada y estadística.

En consecuencia, los resultados del estudio deben interpretarse como un diagnóstico descriptivo robusto de las organizaciones participantes, que permite identificar patrones, brechas y tendencias relevantes en materia de ciberseguridad, sin que ello implique una inferencia probabilística estricta sobre la totalidad del país.

De igual forma es importante indicar, que el enfoque metodológico adoptado busca equilibrar la necesidad de control interno de calidad de los datos con el resguardo de la confidencialidad de las organizaciones participantes. Este diseño contribuye a reducir riesgos asociados a la deseabilidad social y favorece respuestas más abiertas y representativas de la realidad institucional, al tiempo que protege información sensible y estratégica.

3.2. Hallazgos

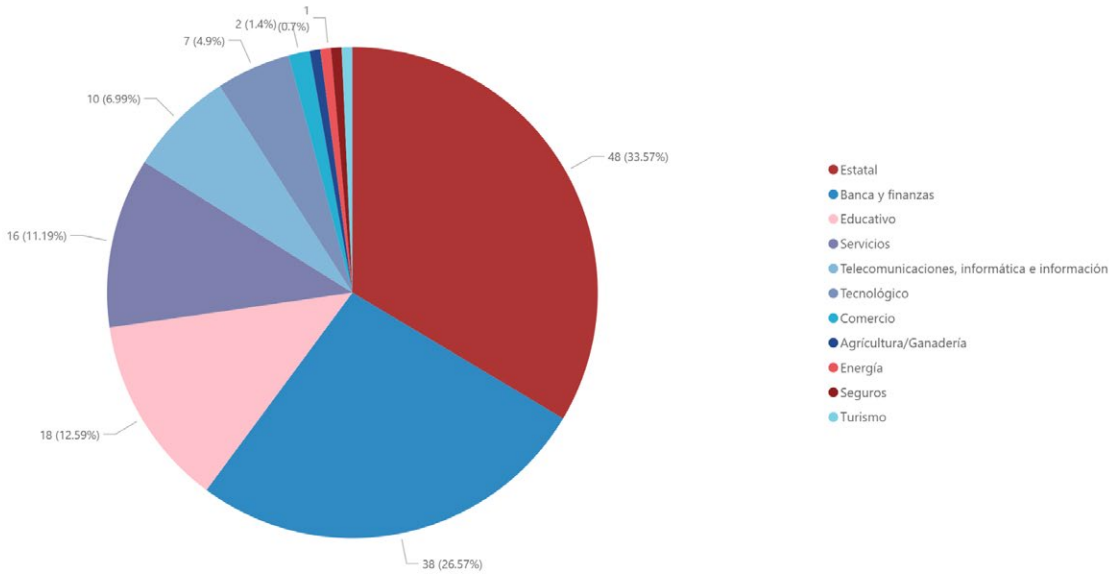
Seguidamente, se presentan los resultados obtenidos en la edición 2025 de la encuesta, en la cual se recopilaron 143 respuestas provenientes de diversos actores institucionales, aportando información relevante sobre los sectores en los que desarrollan sus actividades. Las comparaciones interanuales presentadas en este informe deben entenderse como un ejercicio de análisis de tendencias aproximadas, sustentado en mediciones sucesivas con muestras independientes, lo que permite identificar señales persistentes y patrones estructurales, pero no establecer inferencias causales ni conclusiones longitudinales estrictas.

En este período se evidencia un incremento significativo en la participación respecto a 2024, pasando de 29 a 143 respuestas, lo que representa una participación cercana a cinco veces mayor respecto a la edición anterior. Este crecimiento se atribuye a las mejoras implementadas en las estrategias de comunicación y acompañamiento, así como al aumento de la madurez y del alcance del informe, permitiendo contar con una base de datos más amplia y robusta para el análisis.

La encuesta muestra una amplia representación sectorial. El sector estatal continúa liderando la participación con un 33,57 %, al igual que en 2024, lo que ratifica el compromiso sostenido de las instituciones públicas con los procesos de diagnóstico y evaluación sobre el estado de la ciberseguridad en Costa Rica. En segundo lugar, destaca el sector de banca y finanzas con un 26,57 %, cuya presencia aumentó considerablemente en comparación con ediciones previas; lo anterior resulta especialmente relevante dada la importancia estratégica de este sector en materia de ciberseguridad.

Asimismo, se registró la participación de otros sectores con contribuciones significativas, entre ellos el sector educativo con un 12,59 %, que reafirma el interés de la academia en temas de investigación y desarrollo en tecnología; el sector servicios con un 11,19 %; y el sector de telecomunicaciones, informática e información con un 6,99 %, cuya participación continúa siendo clave en el panorama nacional.

Gráfico 1. Distribución de resultados por sector



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

3.2.1. Estado de la Investigación y Desarrollo en Ciberseguridad

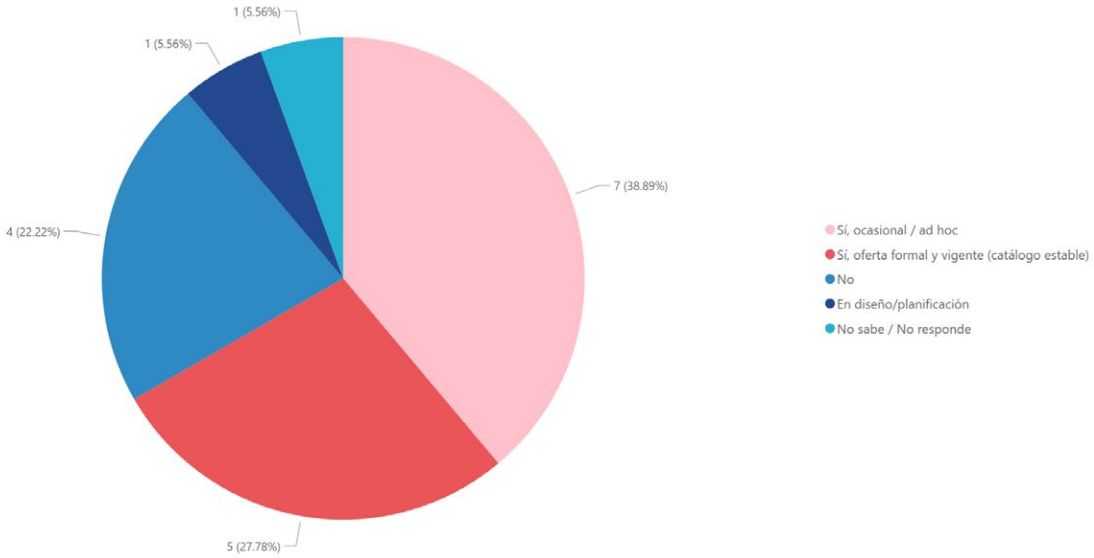
La presente sección se dirige específicamente a la investigación y el desarrollo de la ciberseguridad en instituciones académicas costarricenses. Su propósito es identificar la existencia de iniciativas, programas y mecanismos que impulsen la formación y el fortalecimiento de capacidades en esta área estratégica. En esta edición, el sector educativo mantiene un papel relevante dentro de la muestra, al aportar un 12,59 % de las respuestas. A continuación, se presenta una visión detallada sobre las iniciativas, proyectos y programas en materia de ciberseguridad desarrollados en las instituciones educativas.

En cuanto a la oferta de programas de formación o cursos específicos en ciberseguridad, los resultados muestran un panorama heterogéneo. Solo el 27,78 % de las instituciones declara contar con ofertas consolidadas en esta materia, mientras que la mayoría se sitúa en esquemas de formación no sistemática: un 38,89 % ofrece cursos ocasionales y un 22,22 % aún no dispone de iniciativas formativas específicas en el área. Este patrón refleja, por un lado, un interés sostenido por incorporar la ciberseguridad en la oferta académica y de capacitación; pero, por otro, pone de manifiesto diferencias marcadas en el grado de institucionalización y estabilidad de estas acciones entre organizaciones.

Si bien el informe presenta comparaciones con las ediciones 2023 y 2024, es importante señalar que las variaciones observadas entre años deben interpretarse con cautela. Las diferencias en el tamaño muestral y, especialmente, en la composición sectorial de las organizaciones participantes pueden incidir en los resultados, por lo que no todas las variaciones reflejan necesariamente cambios estructurales en la situación nacional de la ciberseguridad, sino también cambios en la conformación de la muestra analizada.

Si se observa la serie 2023–2025, se confirma una reducción en la proporción de instituciones con programas formales consolidados, acompañada en 2025 por una mayor diversidad de formatos y niveles de avance. Con la información disponible, no es posible determinar plenamente si esta diversidad obedece a un proceso de reconfiguración positiva de la oferta académica o, más bien, a la incorporación en la muestra de instituciones que se encuentran en etapas iniciales de desarrollo de sus capacidades formativas en ciberseguridad.

Gráfico 2. Oferta de programas de formación o cursos específicos en ciberseguridad en instituciones educativas (orientados a desarrollo de capacidades técnicas y/o I+D)



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

Al respecto, las personas participantes detallaron los siguientes programas o cursos ofrecidos actualmente en sus instituciones educativas:

- Se ofrece Maestría Profesional en Ciberseguridad, así como cursos libres y técnicos en esta área (por ejemplo, *hacker* ético).
- Introduction to Cybersecurity.

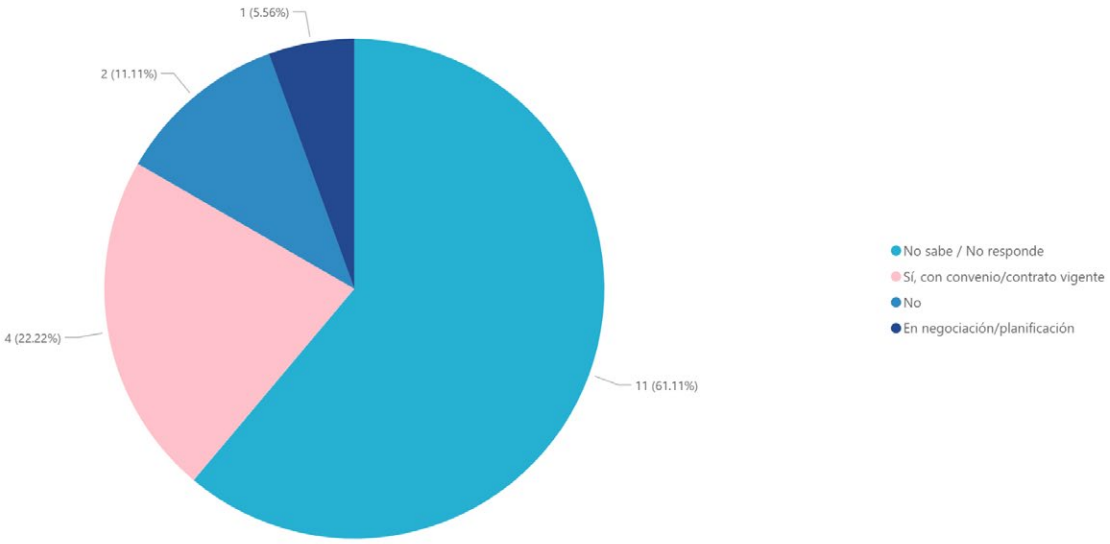
- Conceptos y principios de ciberseguridad.
- Especialización en ciberseguridad.
- Ciberseguridad del MICITT.
- Licenciatura en Ingeniería en Ciberseguridad.
- Protección de dispositivos y *software* seguro; seguridad en el trabajo remoto y *phishing*; ingeniería social y privacidad.
- Capacitación en NIST.
- Los propuestos por el MICITT.
- Ciberseguridad del 1 al 3.
- Cursos básicos internos y otros básicos con el apoyo de fabricantes, además de la formación académica formal.
- Cursos del MICITT.

En conjunto, esta información permite afirmar que una mayoría de instituciones participantes cuenta con iniciativas formativas relacionadas con la ciberseguridad. Este compromiso resulta fundamental para fortalecer la preparación del talento nacional y contribuir al desarrollo de un ecosistema capaz de enfrentar los desafíos emergentes en materia de seguridad digital.

Respecto a los convenios con instituciones o empresas para la formación en ciberseguridad, los resultados de 2025 muestran un escenario distinto al de los años anteriores. En la edición 2023, un 81,8 % de las instituciones afirmaba mantener convenios activos, mientras que en 2024 esta cifra descendió al 60 %, reflejando una disminución notable en la colaboración interinstitucional. En contraste, los resultados de 2025 presentan una distribución mucho más dispersa: la mayoría de las personas encuestadas indicó desconocer si su institución cuenta con convenios vigentes, mientras que un grupo menor confirmó mantener alianzas activas y otras señalaron no contar con ellas o estar en proceso de negociación.

El incremento en las respuestas «no sabe/no responde», que en esta edición representa el 61,11 % del total, supera ampliamente lo observado en 2023 y 2024. Este comportamiento puede interpretarse como un indicador de poca comunicación interna o de falta de claridad institucional respecto a la gestión de alianzas en ciberseguridad. Aunque sí existen instituciones que mantienen convenios vigentes, la baja visibilidad de estas iniciativas entre el personal participante sugiere que los esfuerzos de colaboración no siempre se comunican o articulan de manera efectiva.

Gráfico 3. Convenios/alianzas vigentes con otras organizaciones para la formación en ciberseguridad (docencia, capacitación, pasantías o codesarrollo)



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

Lo anterior permite concluir que el panorama de 2025 no evidencia necesariamente una disminución en la existencia de convenios, sino más bien una creciente falta de claridad respecto de su vigencia, alcance y contenidos. Este resultado sugiere que el problema no radica únicamente en la ausencia de alianzas, sino en su limitada visibilidad dentro de las propias instituciones. En consecuencia, se refuerza la necesidad de fortalecer la comunicación interna y los mecanismos de registro y seguimiento de estas colaboraciones, dado que continúan siendo un recurso clave para el desarrollo de capacidades en ciberseguridad y para la articulación de esfuerzos entre academia, sector público y sector privado.

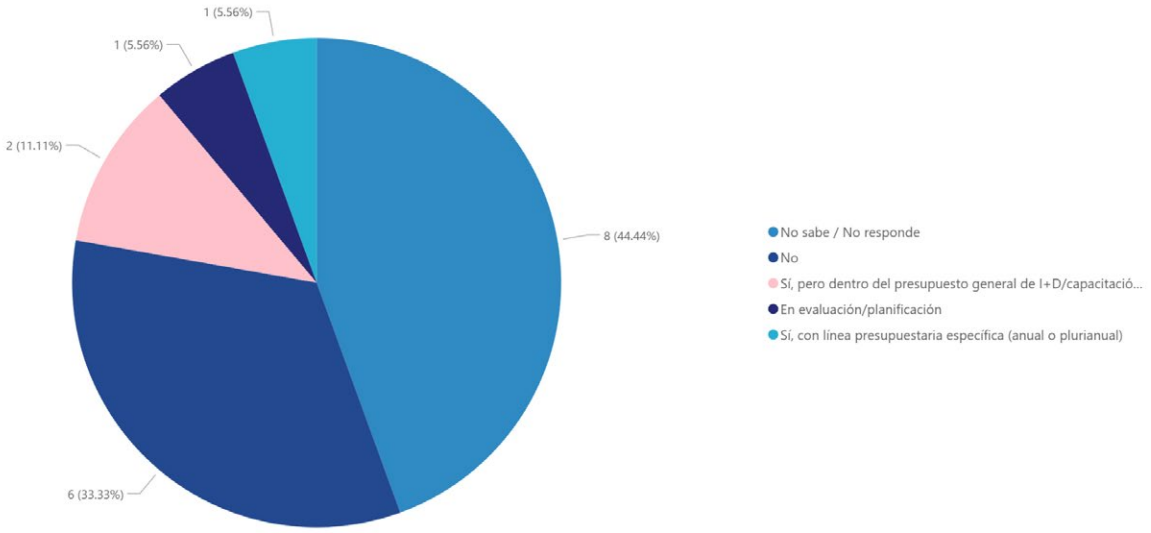
Por otra parte, entre las instituciones que sí cuentan con convenios, la percepción sobre su efectividad continúa siendo positiva: la totalidad de estas instituciones evaluó sus convenios como efectivos (50 %) o muy efectivos (50 %), lo que evidencia beneficios concretos cuando estas alianzas se gestionan e implementan adecuadamente.

En cuanto a la disponibilidad de presupuesto dedicado a actividades de investigación y desarrollo (I+D) en ciberseguridad, los resultados de 2025 muestran un comportamiento distinto al observado en 2023 y 2024. Mientras que en esas ediciones se había evidenciado una disminución significativa en la asignación de recursos específicos, al pasar de un 54,5 % de respuestas afirmativas en 2023 a un 20 % en 2024, este año la tendencia no se centra tanto en la reducción del financiamiento,

sino en la falta de claridad interna al respecto. La proporción más alta de respuestas corresponde a personas que manifestaron no saber si existe un presupuesto asignado (44,44 %), seguida por quienes indicaron que su institución no cuenta con financiamiento específico (33,33 %). Solo un grupo reducido señaló disponer de un presupuesto dedicado o de recursos incorporados dentro de líneas generales de investigación y desarrollo o capacitación.

Esta distribución revela que persisten desafíos importantes en la gestión presupuestaria para ciberseguridad. Si bien es evidente que la ausencia de presupuesto específico continúa afectando a muchas instituciones, la elevada cantidad de respuestas «no sabe/no responde» sugiere que no siempre existe una comunicación clara sobre cómo se asignan o administran los recursos destinados a estas actividades. En algunos casos, esto podría asociarse con estructuras presupuestarias complejas; en otros, con una integración insuficiente de la ciberseguridad dentro de las prioridades estratégicas institucionales.

Gráfico 4. Presupuesto dedicado para actividades de investigación y desarrollo (I+D) en ciberseguridad



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

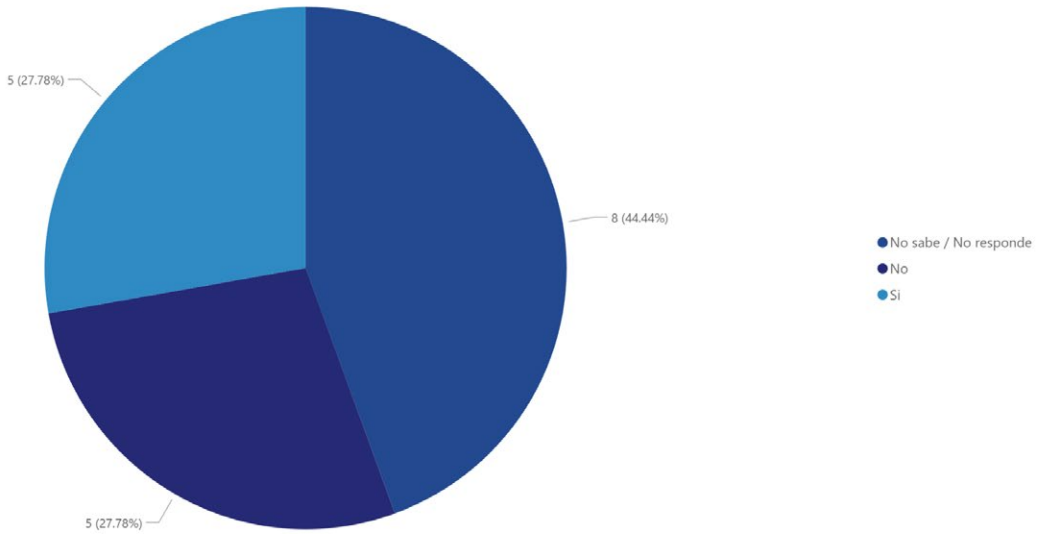
A partir de lo anterior, los resultados de 2025 no permiten concluir, por sí solos, una reducción del financiamiento, sino más bien una menor visibilidad sobre la existencia de estos recursos. Esto plantea la necesidad de reforzar la transparencia y la comunicación interna sobre la asignación presupuestaria en ciberseguridad, especialmente cuando se trata de un área estratégica para la continuidad operativa y el fortalecimiento de la seguridad digital.

En línea con lo analizado previamente, los resultados de 2025 introducen un matiz distinto respecto de la ejecución de proyectos de investigación en ciberseguridad. Mientras que en 2023 y 2024 era posible identificar una tendencia relativamente clara de disminución en la proporción de instituciones que reportaban actividades investigativas, en esta edición dicho comportamiento se vuelve menos nítido debido al elevado porcentaje de personas encuestadas que manifiestan no saber si, en los últimos 12 meses, su institución llevó a cabo proyectos de investigación en este ámbito.

Entre quienes sí tienen claridad sobre el tema, un 27,78 % indicó que su institución ha ejecutado proyectos de investigación, mientras que otro grupo, con el mismo porcentaje, señaló que no se realizaron. Esta distribución sugiere que, más allá de un descenso en la actividad investigativa, existe una falta de visibilidad o comunicación interna respecto a las iniciativas de investigación en ciberseguridad; lo anterior se refleja en el 44,44 % que indica no tener conocimiento al respecto.

Este predominio de respuestas «no sabe/no responde» también podría estar asociado a desafíos identificados en preguntas previas, como la falta de financiamiento o la ausencia de líneas presupuestarias claras, factores que históricamente han limitado la capacidad de las instituciones para impulsar proyectos de investigación. La poca claridad interna sobre estas actividades podría, además, generar una percepción de menor importancia o prioridad de la investigación en ciberseguridad, lo que afectaría la continuidad y el desarrollo de iniciativas en este campo.

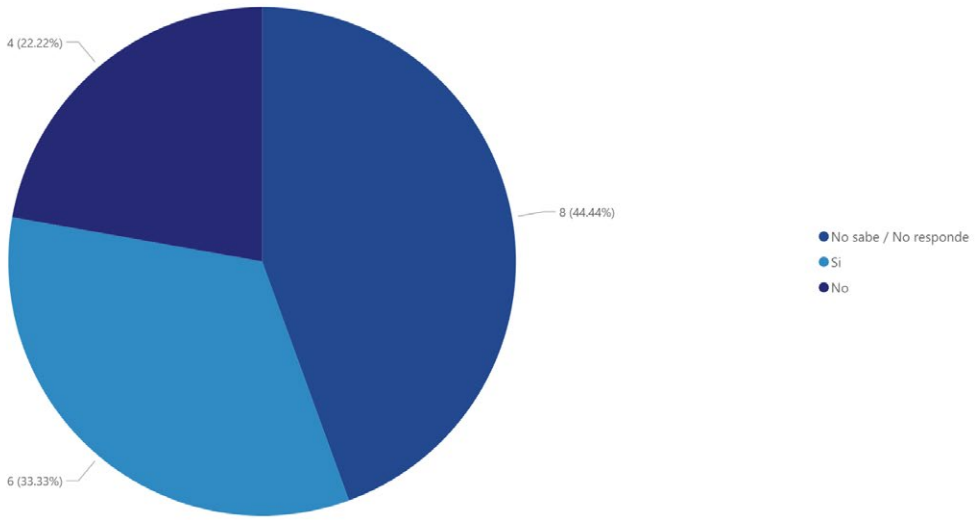
Gráfico 5. En los últimos 12 meses, la institución ha ejecutado proyectos de investigación en ciberseguridad



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

En complemento, se consultó si en los últimos 12 meses las instituciones han formulado proyectos de investigación en ciberseguridad o tienen intención de hacerlo. Los resultados muestran datos mixtos: un tercio de las personas encuestadas indicó que sí existe formulación o intención de formular proyectos (33,33 %), mientras que un grupo menor señaló que no (22,22 %). Sin embargo, casi la mitad (44,4 %) manifestó no saber o no responder, lo que vuelve a evidenciar un nivel importante de incertidumbre interna respecto a la planificación de la investigación en ciberseguridad dentro de las organizaciones.

Gráfico 6. En los últimos 12 meses, la institución ha formulado proyectos de investigación en ciberseguridad o tiene intención de formularlo



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

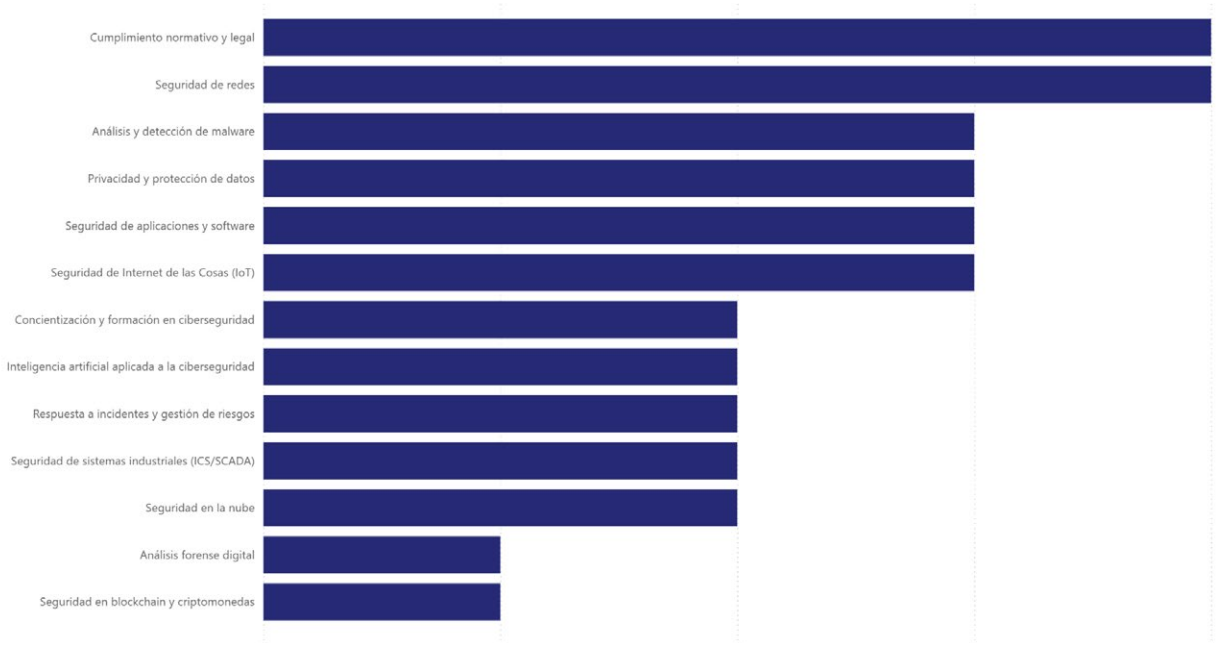
Entre las instituciones que indicaron haber formulado proyectos o tener la intención de hacerlo, la mayoría señaló que estos abarcan tanto investigación como desarrollo (66,67 %), mientras que el 33,33 % restante se concentra exclusivamente en investigación. No se registraron casos de proyectos dedicados únicamente al desarrollo, lo que sugiere que, aunque existen esfuerzos por articular iniciativas en ciberseguridad, estos continúan fuertemente orientados desde una perspectiva académica o teórica, con menor presencia de proyectos centrados exclusivamente en la creación de soluciones aplicadas o tecnologías específicas.

Asimismo, los datos recopilados en esta edición permiten identificar prioridades claras respecto a las áreas en las que actualmente se concentran los esfuerzos de investigación y desarrollo (I+D) en ciberseguridad. Este año, el cumplimiento normativo y legal destaca como el ámbito más atendido, al ser seleccionado por el

80 % de las instituciones que reportaron actividades de I+D. Este predominio sugiere una creciente preocupación por fortalecer marcos regulatorios, políticas internas y procesos de cumplimiento frente a un entorno normativo cada vez más exigente.

A continuación, se presenta un conjunto de áreas de investigación y desarrollo con niveles de participación similares, cada una reportada por el 60 % de las instituciones: seguridad de redes; seguridad de aplicaciones y *software*; Internet de las Cosas (IoT); seguridad de sistemas industriales (ICS/SCADA); análisis y detección de *malware*; respuesta a incidentes; y gestión de riesgos, privacidad y protección de datos. La presencia uniforme de estas áreas evidencia que los esfuerzos institucionales siguen orientados tanto a pilares tradicionales de la ciberseguridad como a la protección de infraestructuras tecnológicas críticas y a la gestión de riesgos operativos.

Gráfico 7. Áreas específicas de ciberseguridad en las que se enfocan las investigaciones y desarrollo



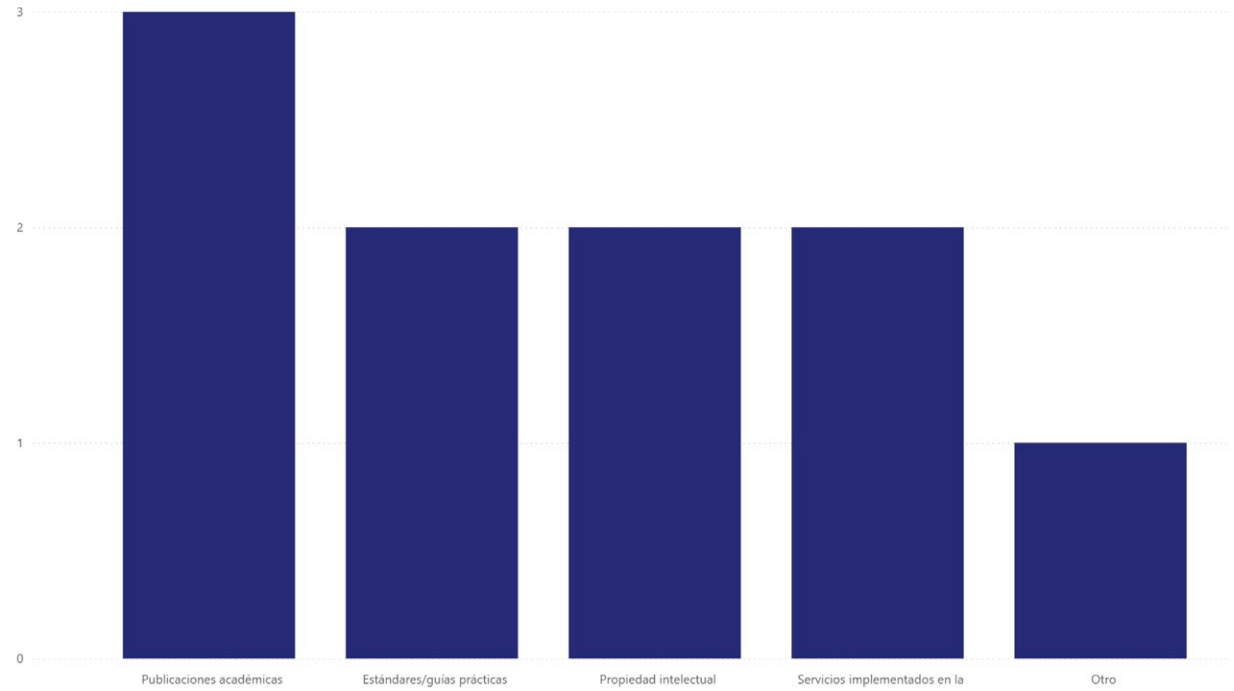
Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

Por otra parte, áreas emergentes como seguridad en la nube, inteligencia artificial aplicada a la ciberseguridad, seguridad en *blockchain* y criptomonedas, y análisis forense digital registran participaciones más bajas, cada una con un 20 %. Aunque estos temas han ganado relevancia internacional, los resultados de 2025 reflejan que aún no se han posicionado como prioridades en la mayoría de las instituciones. Esta menor presencia podría asociarse con una adopción más lenta de estas tecnologías, falta de personal especializado o recursos limitados para investigar en ámbitos avanzados.

Podemos indicar que los resultados de 2025 muestran un enfoque diversificado en la investigación institucional, aunque con un énfasis más fuerte en áreas regulatorias y operativas. No obstante, persisten brechas en temáticas emergentes que serán claves para enfrentar desafíos futuros. Integrar gradualmente áreas como inteligencia artificial, blockchain, análisis forense digital o seguridad en la nube podría fortalecer la capacidad nacional para adaptarse a un entorno tecnológico en rápida evolución.

En cuanto a los productos tangibles generados a partir de actividades de investigación y desarrollo en ciberseguridad durante los últimos 12 meses, los resultados de la edición 2025 muestran una producción moderada y concentrada en un conjunto específico de entregables. Entre las instituciones que reportaron resultados, se observa que las publicaciones académicas, la propiedad intelectual, los servicios implementados y las guías o estándares prácticos fueron los productos más frecuentes, cada uno registrado por el 40 % de las respuestas. Esto refleja que, cuando existen esfuerzos de investigación, estos suelen orientarse hacia la generación de conocimiento formal, documentación técnica o servicios aplicables dentro de las propias instituciones.

Gráfico 8. Productos tangibles ha generado la investigación + desarrollo en ciberseguridad en los últimos 12 meses



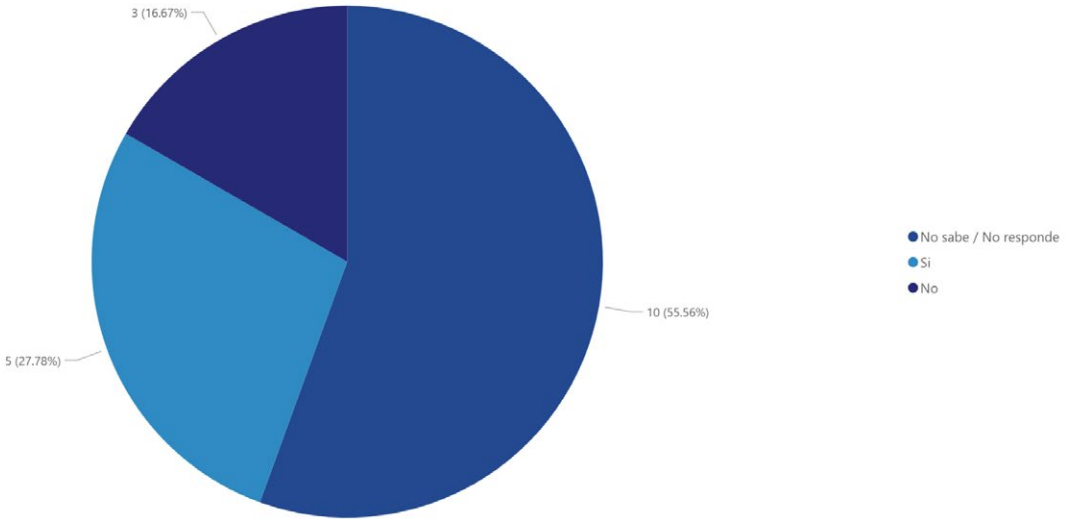
Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

Por otra parte, categorías como el desarrollo de prototipos o *software* especializado y la obtención de patentes no registraron resultados en esta edición, lo cual evidencia una menor presencia de iniciativas orientadas a la innovación tecnológica aplicada.

Finalmente, un 20 % de las respuestas señaló la categoría «otro», lo que indica la existencia de productos menos comunes o no contemplados explícitamente en la lista, aunque su presencia es marginal en comparación con los elementos principales. En conjunto, los resultados sugieren que las instituciones continúan generando aportes valiosos en términos de documentación, normativas internas y servicios institucionales; sin embargo, persisten desafíos para avanzar hacia productos más innovadores como prototipos, herramientas tecnológicas o desarrollos con potencial de protección intelectual formal.

Desde otra óptica, en lo que respecta a los planes futuros para realizar proyectos de investigación y desarrollo en ciberseguridad, los resultados de 2025 confirman la tendencia descendente observada en años anteriores. Mientras que en 2023 una mayoría (72,7 %) indicó contar con planes futuros en materia de I+D, este porcentaje se redujo al 50 % en 2024. En la presente edición, la cifra desciende nuevamente, alcanzando únicamente un 27,8 % de instituciones que afirman tener planes a futuro en esta área. Paralelamente, un 16,67 % señaló no contar con planes y, de manera aún más crítica, la mayoría de las personas encuestadas (55,56 %) manifestó desconocer si su institución dispone de alguna estrategia de investigación o desarrollo proyectada. Este último dato sugiere no solo una contracción de la planificación en I+D, sino también déficits en la comunicación interna y en la formalización de dichas estrategias.

Gráfico 9. Planes futuros en términos de investigación y desarrollo en ciberseguridad



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

Este giro de perspectivas puede relacionarse con restricciones de recursos, escasez de personal capacitado o especializado en investigación y desarrollo, o con la primacía de otras prioridades institucionales en la agenda organizacional. La falta de proyección para impulsar esfuerzos en un tema de alta relevancia puede incrementar la dependencia de factores externos al momento de innovar y mantener competitividad frente a otros actores.

Por otra parte, en cuanto a las principales barreras identificadas por las instituciones en términos de investigación y desarrollo en ciberseguridad durante 2025, los resultados muestran un cambio importante respecto a los años anteriores. En esta edición, la escasez de personal calificado se posiciona como el desafío predominante, señalado por el 94,1 % de las personas encuestadas. Este dato evidencia que la falta de talento especializado continúa siendo un obstáculo central que limita la capacidad de las instituciones para desarrollar proyectos de investigación y avanzar en iniciativas técnicas más complejas.

El financiamiento se mantiene como otra de las barreras más relevantes, reportado por el 82,4 % de las instituciones. Si bien este porcentaje es ligeramente menor al registrado en 2024 cuando el 100 % de las instituciones identificaron la falta de financiamiento como el principal impedimento, continúa representando un factor crítico que afecta de manera directa la continuidad y el alcance de las actividades de I+D en ciberseguridad.

En un segundo elemento como barrera señalaron el acceso a datos e infraestructura indicado por el 47,1 %, lo cual continúa reflejando limitaciones estructurales para realizar investigación en entornos reales. Estas restricciones dificultan el desarrollo de estudios avanzados, pruebas, simulaciones y validaciones necesarias para fortalecer las capacidades nacionales en ciberseguridad.

Finalmente, un 35,3 % de las instituciones mencionó la colaboración público-privada o público-público como un desafío, lo que indica que aún persisten barreras para establecer alianzas estratégicas que permitan compartir recursos, conocimientos y capacidades técnicas entre organizaciones.

En conjunto, los resultados de este año revelan que la escasez de personal calificado y la falta de financiamiento suficiente continúan siendo los principales obstáculos para fortalecer la investigación y el desarrollo en ciberseguridad. Aunque algunas de estas barreras ya habían sido señaladas en años anteriores, su persistencia evidencia la necesidad de una estrategia articulada que combine inversión, formación de talento y mecanismos efectivos de colaboración interinstitucional. Sin abordar estos desafíos, el avance de la investigación en ciberseguridad seguirá enfrentando limitaciones que pueden afectar la preparación y resiliencia tecnológica del país.

En cuanto a la relevancia de la investigación y el desarrollo en ciberseguridad en instituciones académicas, las respuestas recibidas en esta edición se mantienen dentro del rango observado en años anteriores. Un 61,11 % de las personas encuestadas considera que la investigación y el desarrollo en esta área es «Muy importante», cifra que se aproxima a los resultados registrados en 2023 (54,5 %) y 2024 (60 %). Esto muestra una tendencia estable en el reconocimiento del valor estratégico que tiene la ciberseguridad en el ámbito académico.

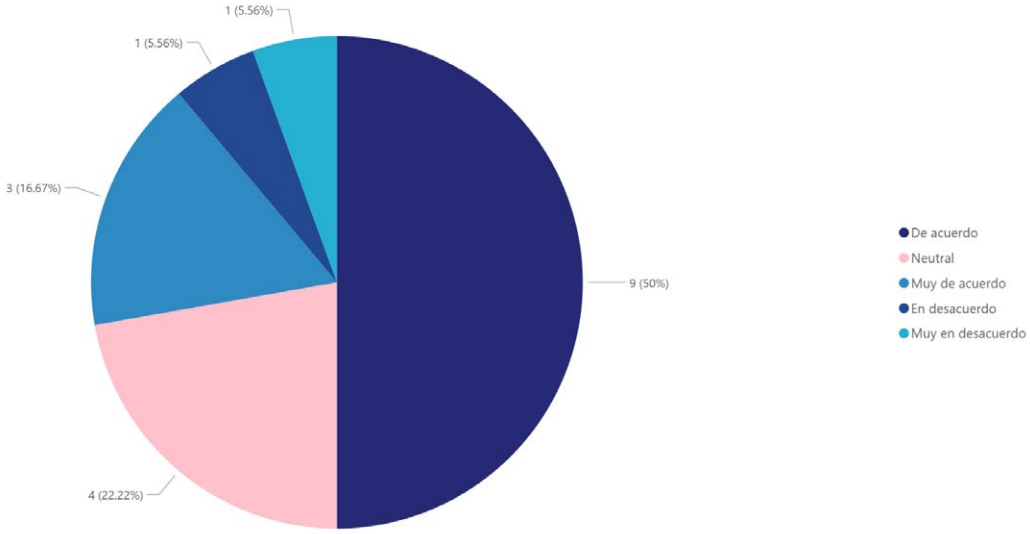
Si bien el análisis evidencia que la mayoría considera este tema como «Muy importante» o «Importante», también resulta relevante señalar que existe un 11,11 % que lo clasifica como «Poco importante», así como una minoría que indica que «No es importante» o que desconoce el nivel de relevancia. Estos resultados subrayan la necesidad de fortalecer la sensibilización y comunicación interna en las instituciones, destacando la importancia de promover esfuerzos de I+D en ciberseguridad para hacer frente a los desafíos actuales del entorno digital.

Con el propósito de comprender la percepción de las personas encuestadas, se consultó sobre la siguiente afirmación:

> *Las actividades de investigación y desarrollo (I+D) en ciberseguridad en las instituciones académicas de Costa Rica se limitan principalmente a los proyectos de fin de carrera de los programas de posgrado.*

Los resultados señalan que la mitad de las personas encuestadas está de acuerdo con que los principales actores en el ámbito de investigación y desarrollo son los proyectos de fin de carrera. Esta percepción es considerablemente menor en comparación con la edición anterior, en la que un 70 % estuvo de acuerdo con la afirmación. Esta disminución podría relacionarse con una mayor visibilidad de otras iniciativas o espacios en los que se están desarrollando actividades de investigación y desarrollo en ciberseguridad.

Gráfico 10. Percepción sobre afirmación sobre I+D limitante en instituciones académicas



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

Asimismo, se observa que un porcentaje adicional manifestó estar «Muy de acuerdo», mientras que un 22,22 % indicó una posición neutral. Esto podría asociarse con falta de conocimiento o con una participación limitada en iniciativas de investigación y desarrollo dentro de sus instituciones. De forma complementaria, se registra un porcentaje reducido de personas que está en «Desacuerdo» o «Muy en desacuerdo» con la afirmación, lo cual evidencia que todavía persiste la percepción de que estas actividades pueden estar vinculadas principalmente a los proyectos de fin de carrera. Estos resultados subrayan la importancia de fomentar y visibilizar proyectos e iniciativas de investigación y desarrollo en ciberseguridad que trasciendan el ámbito de los trabajos finales de posgrado.

Finalmente, en el espacio abierto para comentarios adicionales sobre el estado de la investigación y el desarrollo (I+D) en ciberseguridad dentro de las instituciones, las respuestas obtenidas refuerzan tendencias observadas en preguntas anteriores. Aunque la mayoría de las personas participantes no agregó observaciones, quienes sí lo hicieron señalaron principalmente desconocimiento sobre si su institución realiza gestiones en esta área. Una de las respuestas incluso sugiere que podrían existir iniciativas desde oficinas internas de ciberseguridad, pero que no están siendo difundidas. Esto coincide con la falta de claridad si estas iniciativas se realizan dentro de la empresa o institución, reportada en varias preguntas del cuestionario, y resalta la necesidad de mejorar los mecanismos de comunicación institucional. La ausencia de información accesible no solo limita la percepción del progreso en I+D, sino que también debilita la capacidad de las comunidades académicas para involucrarse, apoyar o impulsar nuevas iniciativas en ciberseguridad.

3.2.2. Situación Jurídica Tecnológica de la Ciberseguridad Nacional

La presente sección tiene como objetivo diagnosticar la situación jurídica de la ciberseguridad nacional desde la perspectiva de las instituciones participantes en la encuesta. Abarca temas clave como ciberseguridad, gestión y prevención de incidentes informáticos, capacitación y formación en ciberseguridad, incorporación de tecnologías emergentes como la inteligencia artificial y asignación de recursos y presupuesto. Para esta edición 2025, el análisis se construye a partir de las respuestas de un total de 143 participantes, lo que permite obtener una visión más amplia en comparación con años anteriores. A continuación, se presenta una lectura detallada del panorama actual de la ciberseguridad en Costa Rica, considerando, además, la evolución de los resultados reportados en las ediciones previas del *Estado de la Ciberseguridad* 2023 y 2024. Es importante reiterar que si bien el informe presenta comparaciones con las ediciones 2023 y 2024, es importante señalar que las variaciones observadas entre años deben interpretarse con cautela. Las diferencias en el tamaño muestral y, especialmente, en la composición sectorial de las organizaciones participantes pueden incidir en los resultados, por lo que no todas las variaciones reflejan necesariamente cambios estructurales en la situación nacional de la ciberseguridad, sino también cambios en la conformación de la muestra analizada.

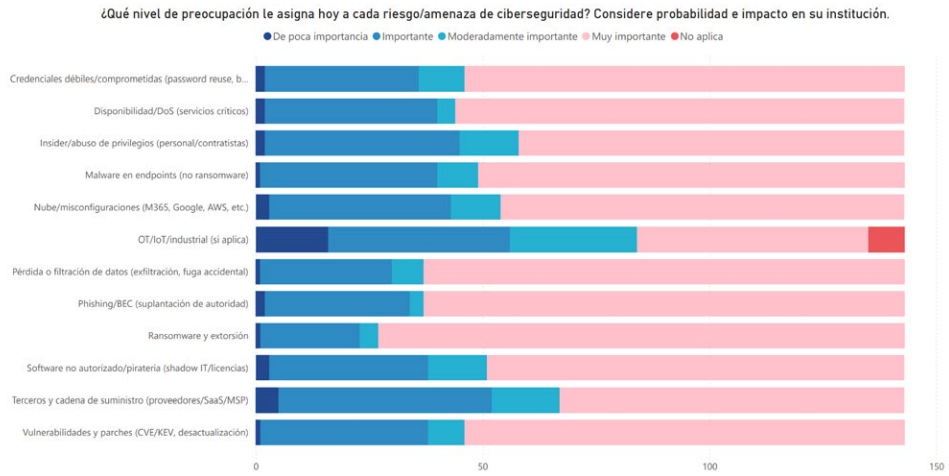
3.2.2.1. Ciberseguridad

En cuanto al nivel de preocupación que las instituciones asignan a los distintos riesgos y amenazas de ciberseguridad, los resultados de la edición 2025 confirman que el *ransomware* y la extorsión continúan siendo la principal amenaza percibida. Este tipo de ataque mantiene su posición como la preocupación más crítica para las organizaciones, tal como ocurrió en 2024, dada su capacidad de paralizar servicios, comprometer información sensible y generar impactos operativos y financieros significativos.

Un segundo grupo de amenazas, con niveles de preocupación muy similares, está compuesto por el *phishing*/BEC (suplantación de autoridad) y la pérdida o filtración de datos, ambos identificados como riesgos altamente relevantes. Estas preocupaciones reflejan la importancia que las instituciones asignan tanto a la protección del factor humano como a la preservación de la integridad y confidencialidad de la información. De forma cercana se encuentra también la preocupación por la disponibilidad de servicios críticos ante ataques de Denegación de Servicios (DoS por sus siglas en inglés), lo cual evidencia que garantizar la continuidad operativa sigue siendo un tema central dentro de la gestión de riesgos de ciberseguridad.

De igual forma, amenazas como las vulnerabilidades de *software* y las credenciales débiles o comprometidas se mantienen entre los factores de mayor atención, lo cual refuerza la necesidad de fortalecer prácticas de actualización, gestión de parches y políticas robustas de autenticación y contraseñas. En contraste, otros riesgos como cadena de suministro, malas configuraciones en la nube, *malware* no asociado a *ransomware*, uso de *software* no autorizado e incidentes internos se ubican en niveles de preocupación relativamente menores. Aun así, su presencia en los resultados confirma que las instituciones reconocen un espectro amplio de amenazas; no obstante, tienden a priorizar aquellas con mayor probabilidad de ocurrencia e impacto directo en la operación y la protección de la información.

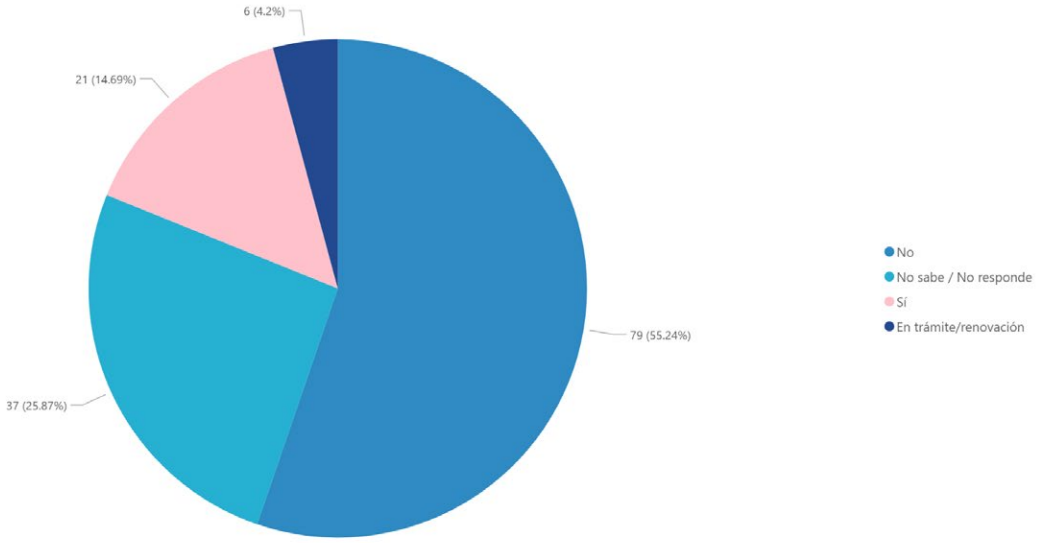
Gráfico 11. Preocupaciones en ciberseguridad



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

Considerando que las amenazas cibernéticas continúan en aumento, más de la mitad de las personas encuestadas indica no contar con una póliza de ciberseguro vigente para cubrir incidentes de seguridad de la información o ciberseguridad (55,24 %). Esto contrasta con el 14,69 % que indica sí contar con este seguro. Además, un 25,87 % señala no tener conocimiento sobre si la institución dispone de dicha póliza.

Gráfico 12. Póliza de ciberseguro vigente para cubrir incidentes de seguridad de la información o ciberseguridad



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

Tomando en consideración que la mayoría de las personas encuestadas indica no tener una póliza de ciberseguro, y que este dato se combina con el nulo interés de contratar un seguro a futuro por parte del 62,94 % de las personas participantes, el resultado sugiere un rezago relevante en esta dimensión de gestión del riesgo. Entre quienes sí contemplan adquirirlo, un 37,74 % no tiene un plazo definido y un 16,98 % se encuentra en etapa de evaluación de posibles pólizas. En conjunto, pese al reconocimiento de las amenazas, las acciones preventivas para fortalecer la resiliencia institucional avanzan con lentitud en este aspecto.

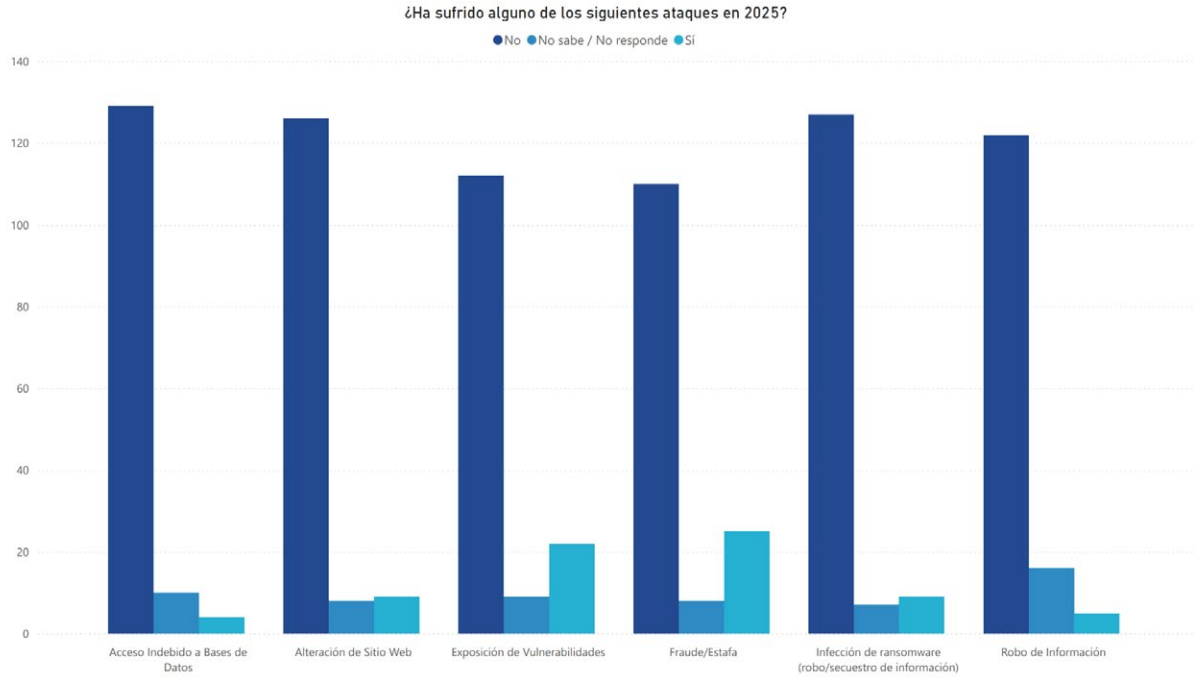
En cuanto a los incidentes cibernéticos sufridos por las instituciones durante 2025, los resultados mantienen una tendencia similar a la de años anteriores: la opción «No» predomina en los tipos de incidentes considerados (infección de *malware* o *ransomware*, fraude o estafa informática, robo de información, exposición de vulnerabilidades, accesos indebidos y alteración de sitios web o servicios), mientras que los casos afirmativos se concentran en una minoría. Llama la atención que los incidentes reportados se concentran sobre todo en fraudes/estafas informáticas y exposición de vulnerabilidades, seguidos por infecciones y alteraciones de servicios; el robo de información y los accesos indebidos presentan menos ocurrencias. También se registra un porcentaje de respuestas de desconocimiento.

Estas respuestas sugieren que, aunque existe una percepción de riesgo elevada frente a amenazas como el *ransomware*, el *phishing* o la pérdida de datos, en la práctica

una proporción menor de instituciones declara haber sido víctima directa de estos eventos en el último año. La presencia de respuestas «no sabe/no responde» en varios tipos de incidentes también indica que, en algunos casos, puede haber limitaciones en los mecanismos de registro o monitoreo de eventos de seguridad, lo que dificulta dimensionar con precisión el impacto real de los ataques cibernéticos.

Con relación con las respuestas ante los incidentes cibernéticos sufridos, los resultados muestran que únicamente un 13,29 % de las personas encuestadas indica que su institución procedió a denunciar el ataque ante el Sistema Judicial. En contraste, un 37,76 % afirma que no se presentó ninguna denuncia. A esto se suma un 48,95 % que señala desconocer si se realizó o no la denuncia, lo que sugiere debilidades de comunicación interna sobre los protocolos posteriores a un ataque y limita la capacidad institucional de seguimiento, además de reducir la visibilidad nacional de este tipo de incidentes.

Gráfico 13. Ataques cibernéticos en 2025



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

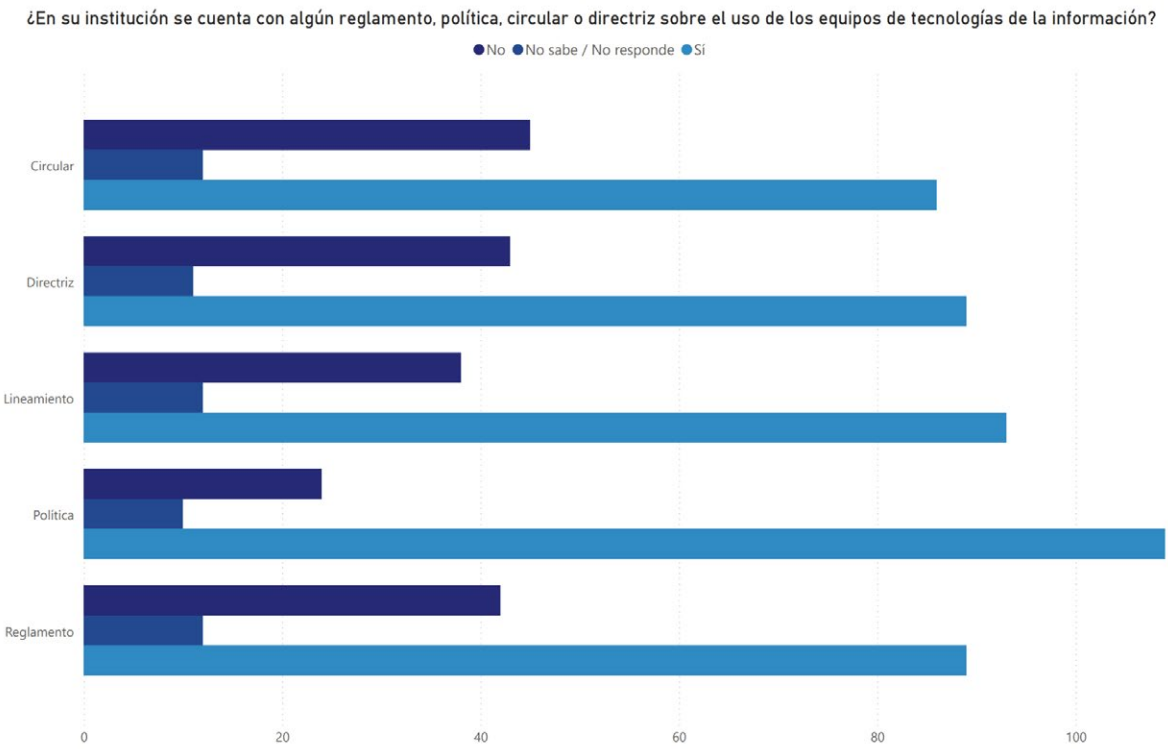
3.2.2.2. Estado de la Ciberseguridad

Con el objetivo de comprender la situación de las organizaciones participantes en materia de ciberseguridad, resulta necesario identificar si cuentan con algún protocolo de actuación ante incidentes en sus sistemas de información. En esta edición, un 76,22 %

de las personas participantes afirma que sí dispone de un manual o procedimiento de actuación ante un ataque o incidente, lo cual refleja un avance importante en la formalización de procesos de respuesta. Este resultado contrasta con el 18,88 % que indica no contar con ningún protocolo, mientras que un porcentaje menor manifiesta desconocer esta información.

En cuanto a la existencia de normativa interna sobre el uso de los equipos de tecnologías de la información, los resultados de 2025 muestran una tendencia hacia la formalización de lineamientos institucionales. La mayoría de las organizaciones indica contar con políticas y reglamentos establecidos, seguidos muy de cerca por lineamientos, directrices y circulares, cada uno con un respaldo mayoritario por parte de las personas encuestadas. Aunque persiste un porcentaje menor que afirma no disponer de estos instrumentos o desconoce su existencia, los datos evidencian que la mayoría de las instituciones ha avanzado en la construcción de un marco normativo que orienta el uso adecuado, seguro y responsable de los recursos tecnológicos, promoviendo prácticas más alineadas con la gestión de riesgos y la protección de la información.

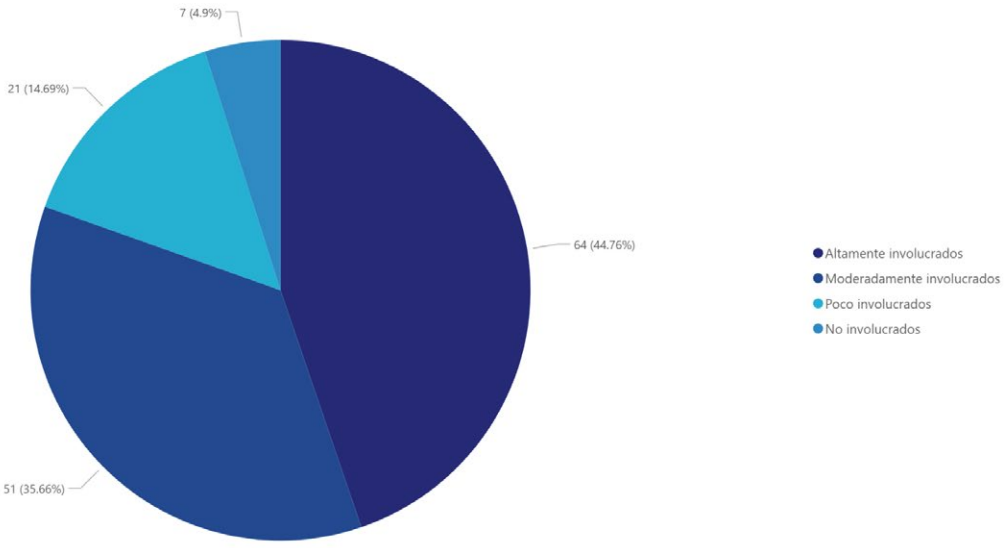
Gráfico 14. La institución cuenta con algún reglamento, política, circular o directriz sobre el uso de los equipos de tecnologías de la información



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

Con relación al nivel de participación de la alta dirección en la gobernanza de la ciberseguridad, las respuestas muestran un incremento en su involucramiento. Mientras que en 2023 y 2024 predominaba la participación moderada como la categoría más frecuente (44 % y 37,9 %, respectivamente), en 2025 el porcentaje de instituciones que reportan una participación alta alcanza el 44,76 %, siendo superior al de 2024 y ligeramente mayor al de 2023. Aun así, tal como ocurría en años anteriores, persiste un grupo significativo con involucramiento limitado: un 35,66 % indica una participación moderada y, aunque disminuye el porcentaje de instituciones con escasa o nula participación, todavía un 14,69 % reporta poco involucramiento. Este contraste evidencia un avance gradual en la integración de la ciberseguridad en la toma de decisiones estratégicas; sin embargo, también subraya que la madurez institucional continúa siendo desigual y requiere fortalecer el compromiso sostenido de la alta dirección para consolidar una gobernanza más robusta.

Gráfico 15. Involucramiento de la alta dirección (Dirección General/Junta) en decisiones y políticas de ciberseguridad

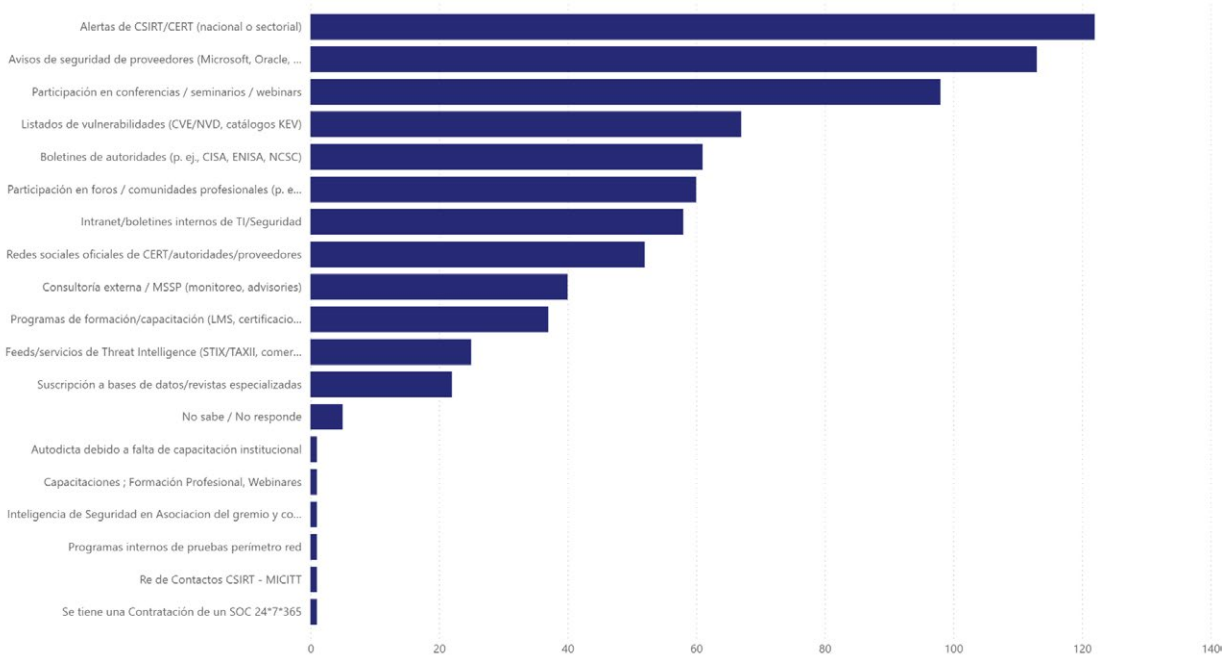


Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

En cuanto a las fuentes que utilizan las instituciones para mantenerse actualizadas sobre tendencias y amenazas en ciberseguridad, los datos muestran una preferencia marcada por los canales más consolidados. Las alertas del CSIRT/CERT nacionales o sectoriales se posicionan como la principal fuente (85,9 %), seguidas por los avisos de seguridad de proveedores (Microsoft, Oracle, Cisco, Fortinet, etc.), con un 79,6 %, lo cual evidencia una fuerte dependencia de alertas oficiales y de fabricantes. Asimismo, la participación en conferencias y seminarios registra un 69 %, lo que refleja

el interés de muchas instituciones por mantenerse actualizadas mediante espacios de intercambio técnico. En otro nivel, los listados de vulnerabilidades alcanzan un 47,2 % de uso y los boletines internos o la intranet institucional llegan a un 40,8 %. En contraste, otras fuentes, como los foros especializados, la consultoría externa o la formación continua, presentan una menor utilización.

Gráfico 16. Fuentes y mecanismos que utiliza la institución para mantenerse actualizada sobre las tendencias y amenazas en ciberseguridad



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

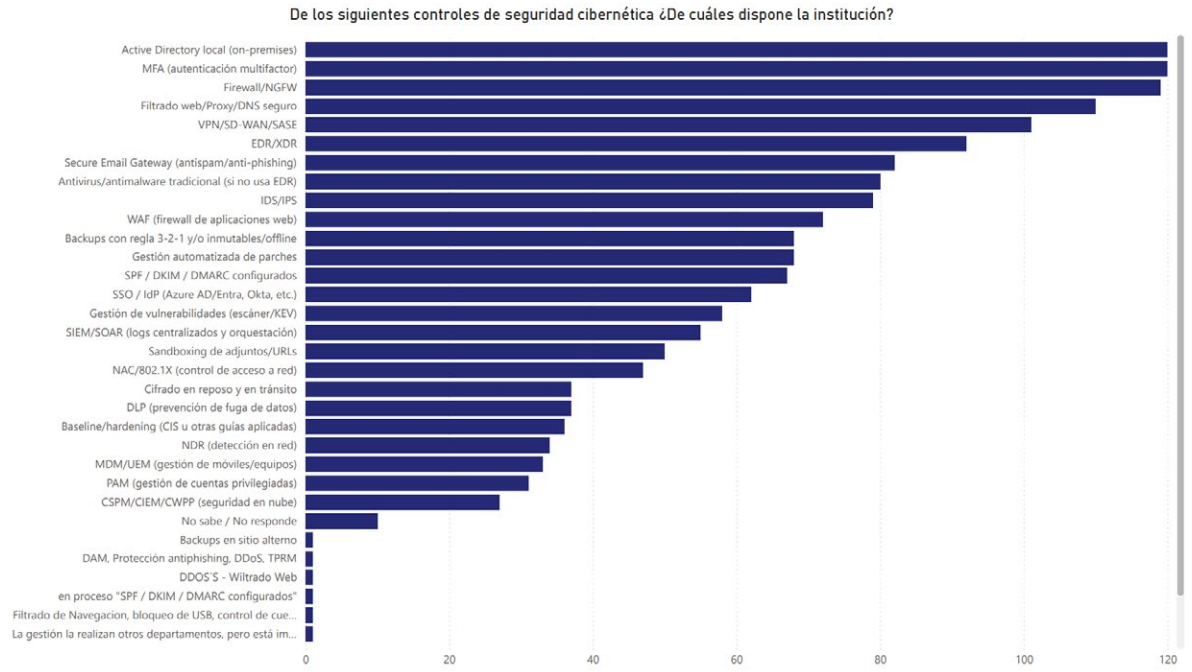
Además, la realización periódica de revisiones sobre el estado de la seguridad de los sistemas de información constituye una buena práctica esencial para garantizar su funcionamiento adecuado y proteger la integridad tanto de los sistemas informáticos como de los datos que procesan. En esta edición, el 79,02 % de las personas encuestadas señala que en su institución se llevan a cabo este tipo de revisiones, consideradas un componente vital de la gestión de la ciberseguridad. No obstante, un 11,89 % manifiesta desconocer si tales controles se realizan y un 9,09 % indica que no se efectúan, lo que evidencia espacios de mejora en la consolidación de mecanismos sistemáticos de supervisión y aseguramiento de la seguridad de la información.

La frecuencia de esta práctica varía entre las instituciones que sí realizan revisiones periódicas. Un 57,52 % indica que mantiene un monitoreo continuo 24/7, lo cual permite una detección más temprana de anomalías. En las demás instituciones,

la periodicidad de estas revisiones difiere; en términos generales, cuanto menor sea el intervalo entre revisiones, mayor será la capacidad de detectar debilidades oportunamente y reducir la exposición a vulnerabilidades frente a posibles ataques cibernéticos.

Además, los resultados muestran nuevamente que la mayoría de las instituciones mantiene una base de controles de ciberseguridad. Entre los mecanismos más utilizados destacan la autenticación multifactor (84,5 %), la gestión de identidades mediante Active Directory (84,5 %), el uso de firewalls/NGFW (83,8 %) y los sistemas de filtrado web y DNS (76,8 %). Estos coinciden con los controles más reportados en las ediciones 2023 y 2024. Asimismo, herramientas como antivirus/*antimalware* (55,6 %), VPN/SD-WAN (71,1 %), EDR/XDR (64,8 %) y soluciones de correo electrónico seguro o antispam (57,7 %) continúan representando pilares fundamentales en la protección institucional.

Gráfico 17. Controles de Ciberseguridad



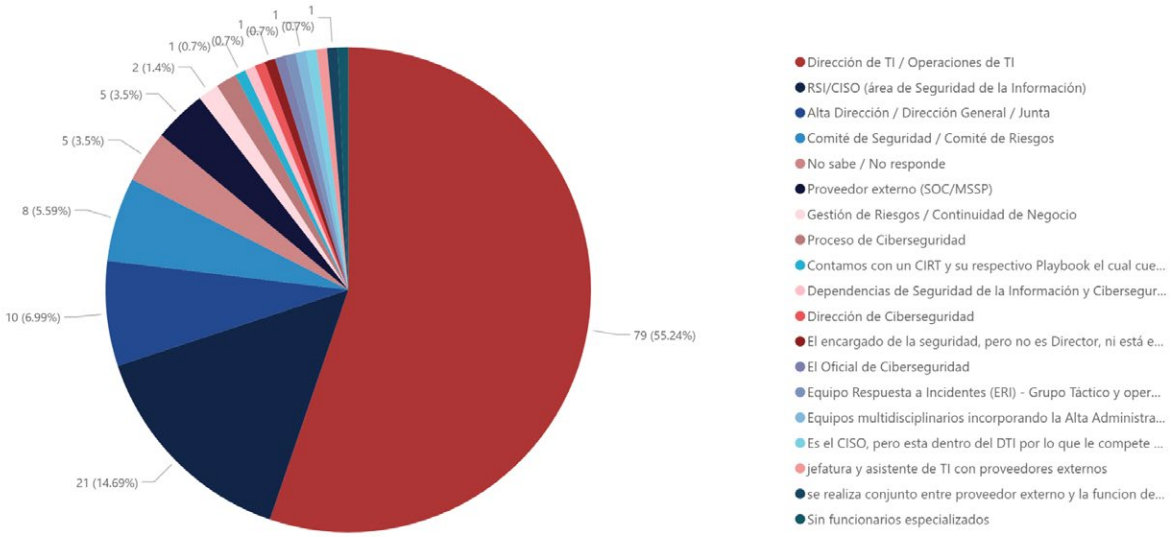
Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

3.2.2.3. Prevención de Incidentes

En comparación con ediciones anteriores, los datos mantienen la tendencia de que la gestión primaria de los incidentes de seguridad de la información recae principalmente en la Dirección de TI u Operaciones de TI, concentrando la mayoría

de las respuestas (55,24 %). Esta cifra reafirma el patrón observado en años previos, en los que TI asumió este rol de responsabilidad. Le sigue el área de Seguridad de la Información o RSI/CISO (14,69 %) y, en menor proporción, la Alta Dirección y los Comités de Seguridad o Riesgos, lo cual refleja una participación todavía limitada de los niveles estratégicos en estos procesos. Si bien estos resultados confirman lo observado en 2023 y 2024, en esta edición se documenta una mayor cantidad de respuestas complementarias que describen escenarios más diversos: instituciones donde la gestión recae en equipos multidisciplinarios, procesos formales de ciberseguridad, CSIRT internos, proveedores externos en conjunto con TI, o incluso casos en los que no existen funcionarios especializados. Estas variaciones evidencian cierta evolución en los modelos de respuesta; sin embargo, persiste una fuerte dependencia del área de TI, lo cual refuerza la necesidad de fortalecer estructuras formales de ciberseguridad y ampliar la participación institucional en la gestión integral de incidentes.

Gráfico 18. Responsable primario de la gestión de incidentes de seguridad de la información (prevención, detección, respuesta y recuperación)



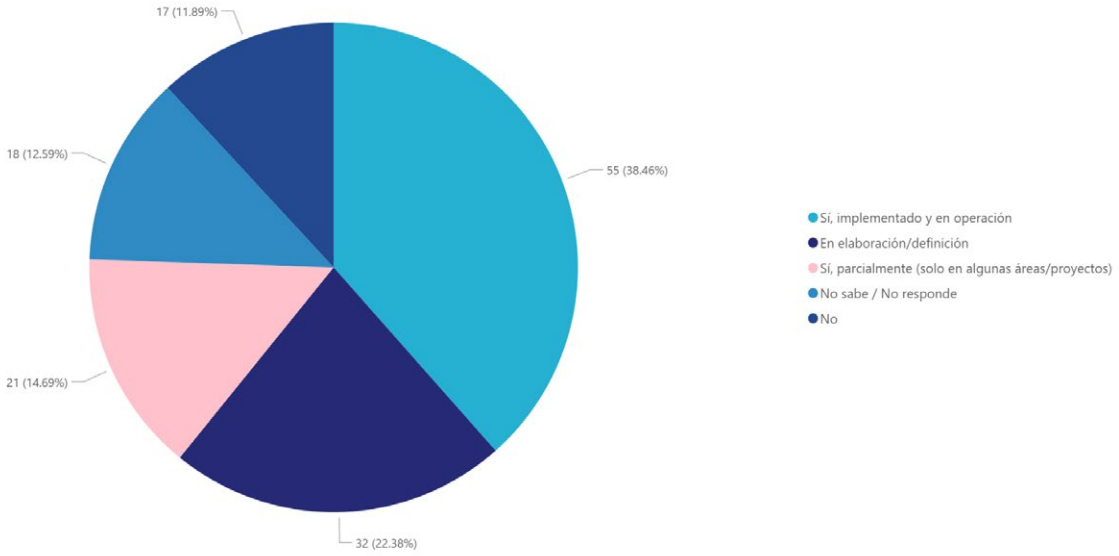
Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

En cuanto a las áreas que participan operativamente en la prevención y respuesta a incidentes, los resultados de esta edición muestran una fuerte centralización de estas tareas en los equipos de TI/Infraestructura y Help Desk, mencionados por el 87,3 % de las personas encuestadas, lo que reafirma su papel como primera línea de atención ante incidentes. Le siguen áreas estratégicas como Seguridad de la Información (48,6 %), proveedores críticos o terceros (42,3 %), SOC/NOC internos o externos (39,4 %) y Gestión de Riesgos y Continuidad de Negocio (35,9 %), lo que evidencia

que la respuesta a incidentes no recae únicamente en departamentos técnicos, sino que involucra a múltiples actores institucionales. También participan, aunque en menor proporción, equipos legales, auditoría interna y áreas de comunicación, lo que sugiere una creciente comprensión de que la gestión de un incidente exige esfuerzos coordinados entre funciones técnicas, administrativas y normativas.

En paralelo, los datos sobre mecanismos de evaluación de riesgo cibernético reflejan una multiplicidad de enfoques. Un 38,46 % de las instituciones cuenta con un mecanismo formal implementado y en operación, mientras que un 22,5 % lo está desarrollando o definiendo. Asimismo, un 14,69 % indica que lo aplica parcialmente y un 12,59 % señala no disponer de mecanismos de evaluación, lo cual puede limitar la capacidad institucional para anticipar, priorizar o mitigar amenazas. Finalmente, un 11,89 % afirma desconocer si su organización utiliza estas herramientas, lo que refuerza la necesidad de comunicación interna y claridad en los procesos de gestión del riesgo cibernético. Si bien se han logrado mejoras, aún quedan puntos débiles por abordar con miras a consolidar una gestión integral del riesgo cibernético.

Gráfico 19. Implementación de mecanismo de evaluación de riesgo cibernético



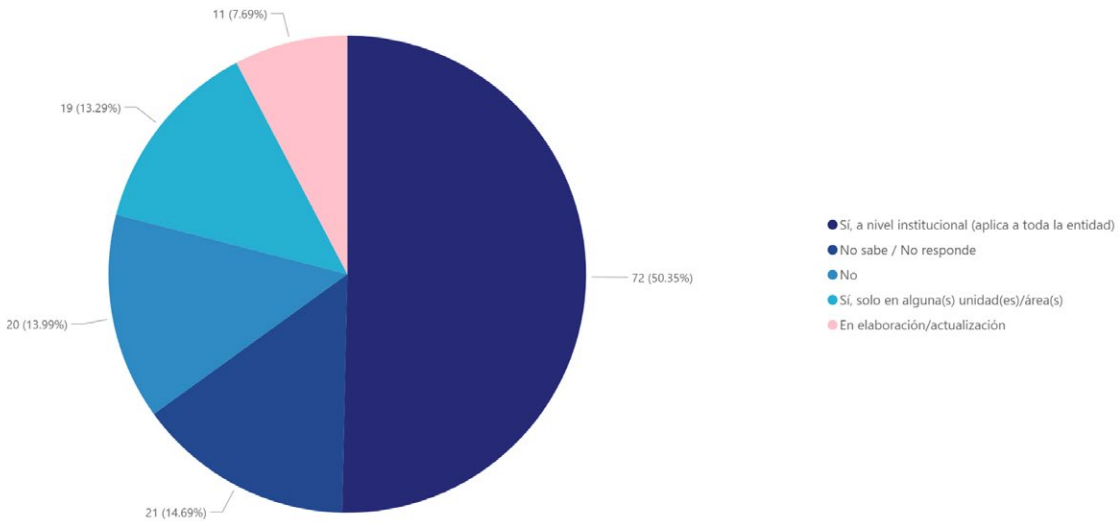
Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

En cuanto al acceso a la red corporativa desde dispositivos personales no gestionados, práctica conocida como Traiga su propio dispositivo (BYOD Bring Your Own Device por sus siglas en inglés), los resultados de la encuesta 2025 muestran que la mayoría de las instituciones mantiene políticas restrictivas. Un 55,94 % prohíbe completamente el acceso de dispositivos personales a la red corporativa, mientras que un 19,58 % lo

permite solo bajo controles específicos, como NAC (Network Access Control, o control de acceso a la red), verificación de postura o acceso condicionado. Únicamente un 6,29 % permite el acceso sin restricciones y un 9,79 % señala que esta política no aplica porque la institución opera únicamente con equipos corporativos. Estos datos reflejan una postura orientada a reducir riesgos asociados al uso de dispositivos no gestionados.

Respecto a la regulación del uso y administración de redes sociales institucionales, el 50,35 % de las personas encuestadas indica que existe una normativa vigente aplicable a toda la institución. Además, un 13,29 % señala que estas directrices se aplican solo en determinadas áreas, mientras que un 7,69 % menciona que se encuentran en proceso de elaboración o actualización. Por otra parte, un 13,99 % indica que no existe ninguna normativa al respecto y un 14,69 % desconoce si la institución cuenta con una. En general, los resultados evidencian avances en la formalización de lineamientos para el uso de plataformas digitales, aunque aún existe espacio para fortalecer y estandarizar estas regulaciones a nivel institucional.

Gráfico 20. Existencia de algún instrumento normativo vigente que regule el uso y administración de redes sociales institucionales

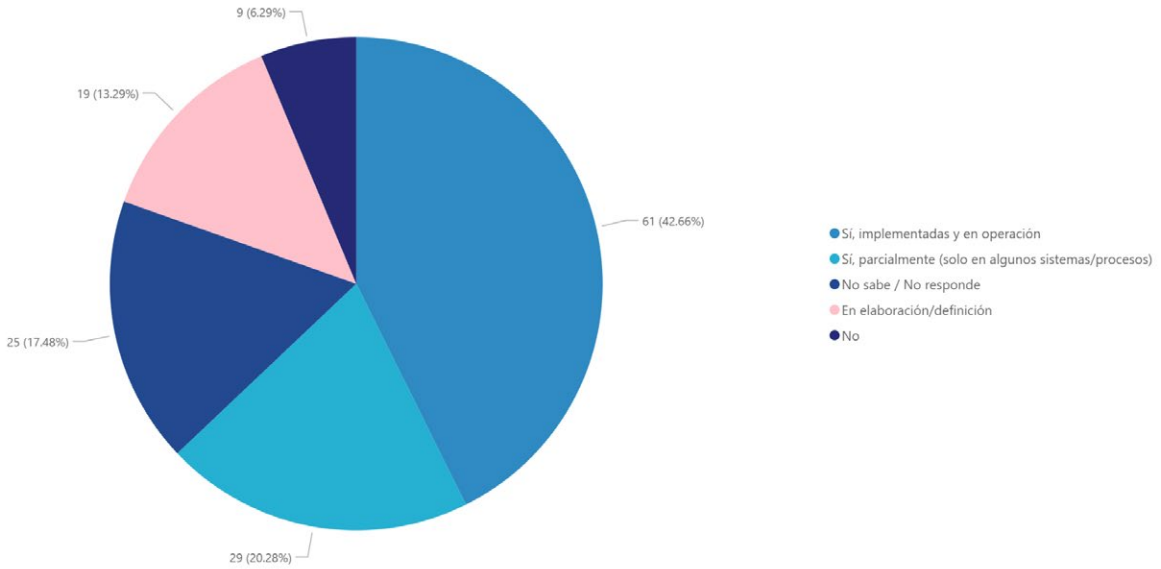


Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

En cuanto a la implementación de medidas técnicas para la protección de datos personales, los resultados muestran un avance significativo respecto a la reducción de la inacción y el desconocimiento: la suma de instituciones que no cuentan con medidas o que desconocen su existencia se ha reducido notablemente a un 23,77 %, frente al 41,3 % del año pasado. Este progreso sugiere una mayor conciencia

sobre la obligatoriedad de la protección de datos. Sin embargo, persisten brechas importantes en la ejecución y finalización de estas medidas. Si bien un 42,66 % de las instituciones indica contar con ellas en operación, una porción considerable aún se encuentra en etapas intermedias o preliminares: un 20,28 % las tiene solo parcialmente implementadas y un 13,29 % se encuentra en proceso de definición.

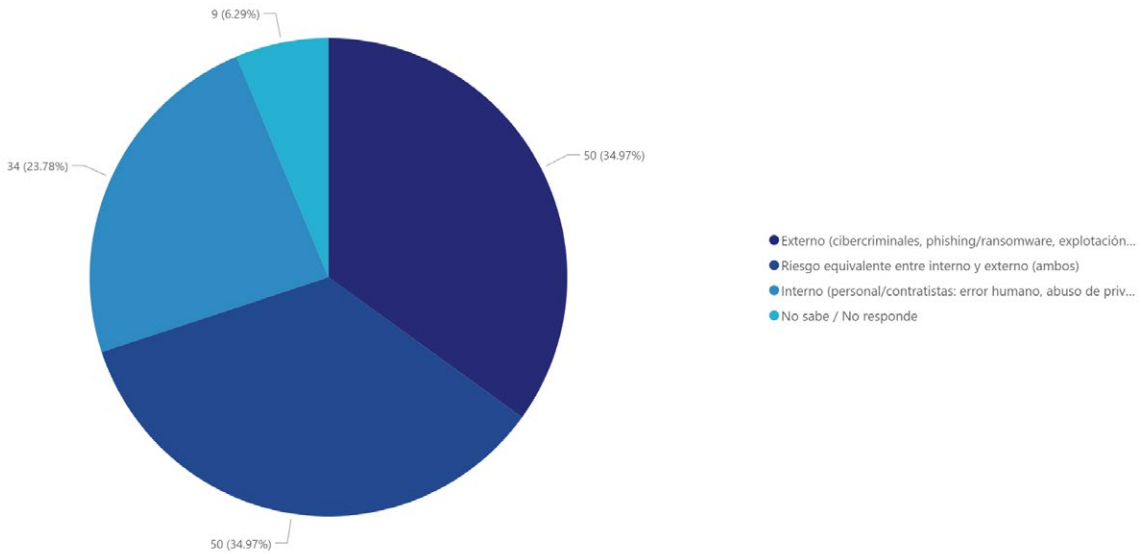
Gráfico 21. Implementación de medidas para el cumplimiento de la ley de protección de datos del cliente



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

Además, en cuanto al origen del riesgo de ciberseguridad percibido por las instituciones, los resultados muestran una distribución amplia. La mayor proporción considera que el riesgo proviene tanto de factores internos como externos, con un 34,97 % que identifica un nivel de riesgo equivalente entre ambos. De manera similar, un 34,97 % señala que las amenazas externas (como ciberdelincuentes, *phishing* o *ransomware*) representan su mayor preocupación, mientras que un 23,78 % percibe que el riesgo principal se ubica en el ámbito interno, asociado a errores humanos, abuso de privilegios o *shadow IT* (TI en la Sombra, se refiere cualquier *software*, *hardware* o recurso de tecnología de la información (TI) utilizado en una red empresarial sin la aprobación, el conocimiento o la supervisión del departamento de Tecnologías de la Información).

Gráfico 22. Origen principal del riesgo de ciberseguridad (probabilidad × impacto) en la institución



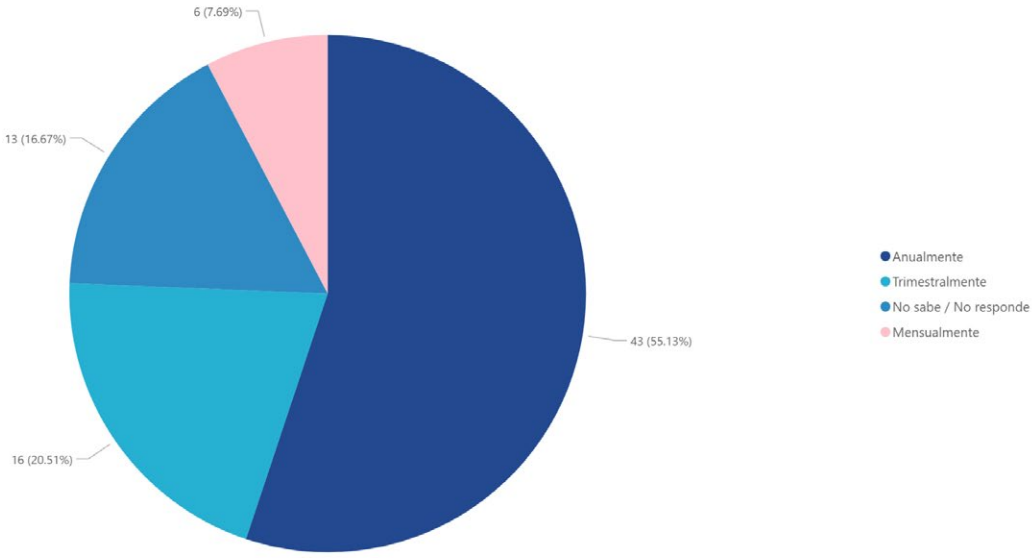
Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

Con respecto al uso de dispositivos de almacenamiento externo en equipos corporativos, los resultados muestran un panorama diverso. Un 31,47 % de las instituciones permite su uso únicamente a personal autorizado, mediante listas blancas o aprobaciones formales, mientras que un 30,77 % aplica una prohibición técnica total (bloqueos en el sistema operativo o soluciones EDR (Endpoint Detection and Response, o Detección y Respuesta en Puntos Finales). Estas constituyen las dos prácticas más utilizadas, aun así, un 14,69 % los permite sin controles y un 11,19 % reconoce que no gestiona formalmente este tipo de dispositivos, lo que evidencia oportunidades de mejora en la protección de la información.

En materia de prácticas para prevenir *phishing* e ingeniería social, las simulaciones de *phishing* y otros ejercicios de ingeniería social continúan siendo un reto para muchas instituciones. Los resultados de esta edición muestran que solo una parte de las organizaciones mantiene prácticas regulares o esporádicas de estos ejercicios (26,57 % y 27,97 %, respectivamente), mientras que un porcentaje aún mayor (34,97 %) reconoce no realizar ningún tipo de simulacro. La inactividad observada evidencia una carencia crítica en la preparación del personal ante ataques basados en engaño. A esto se suma que más de un 10 % del personal no sabe si su institución realiza estas prácticas, lo que muestra una falta de comunicación efectiva sobre las acciones formativas.

Entre las organizaciones que sí aplican simulacros, la frecuencia también revela desafíos. La mayoría los ejecuta únicamente una vez al año (55,13 %), lo que limita el entrenamiento constante frente a técnicas que evolucionan con rapidez. Un grupo menor los realiza trimestralmente (20,51 %), mientras que solo un 7,69 % mantiene ejercicios mensuales. El 16,67 % restante desconoce la periodicidad, lo que nuevamente evidencia que estas actividades, aun cuando existen, no siempre se encuentran debidamente socializadas dentro de las instituciones.

Gráfico 23. Ejecución de simulacros de seguridad

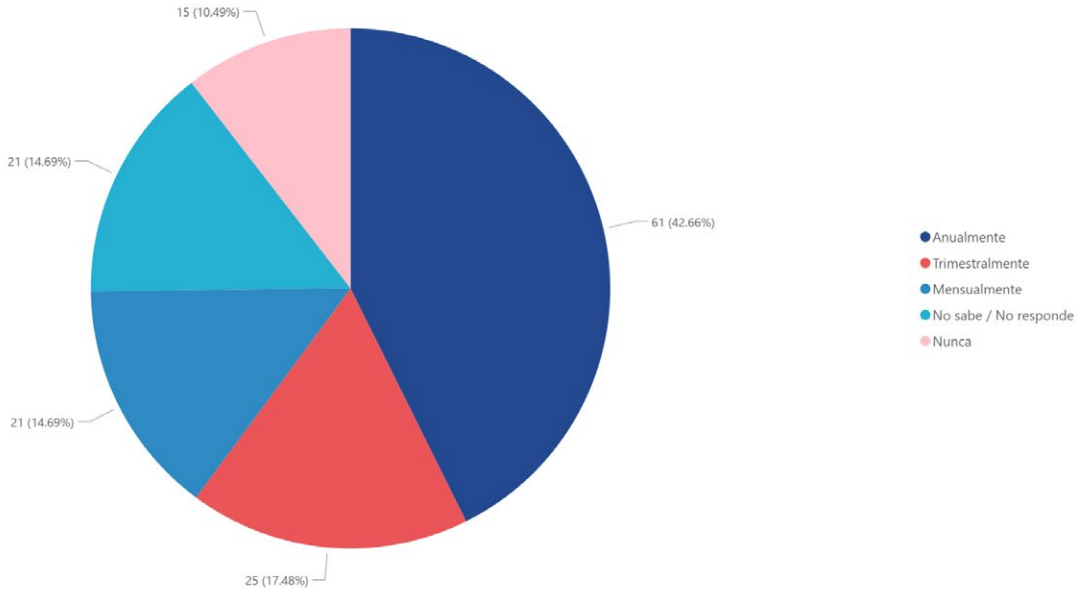


Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

3.2.2.4. Programas de capacitación y/o formación

En materia de formación y capacitación, al analizar la frecuencia con la que la organización participa u organiza eventos como conferencias o talleres sobre ciberseguridad, la mayor proporción se concentra en una periodicidad anual (42,66 %). Se observa una cantidad más reducida de instituciones que los realizan trimestral o mensualmente, y un 10,49 % indica no participar nunca en este tipo de actividades. Este patrón sugiere que, aunque la capacitación en ciberseguridad está presente, en muchos casos podría orientarse más a esfuerzos puntuales que a un proceso continuo de actualización, pese a la evolución permanente de las amenazas.

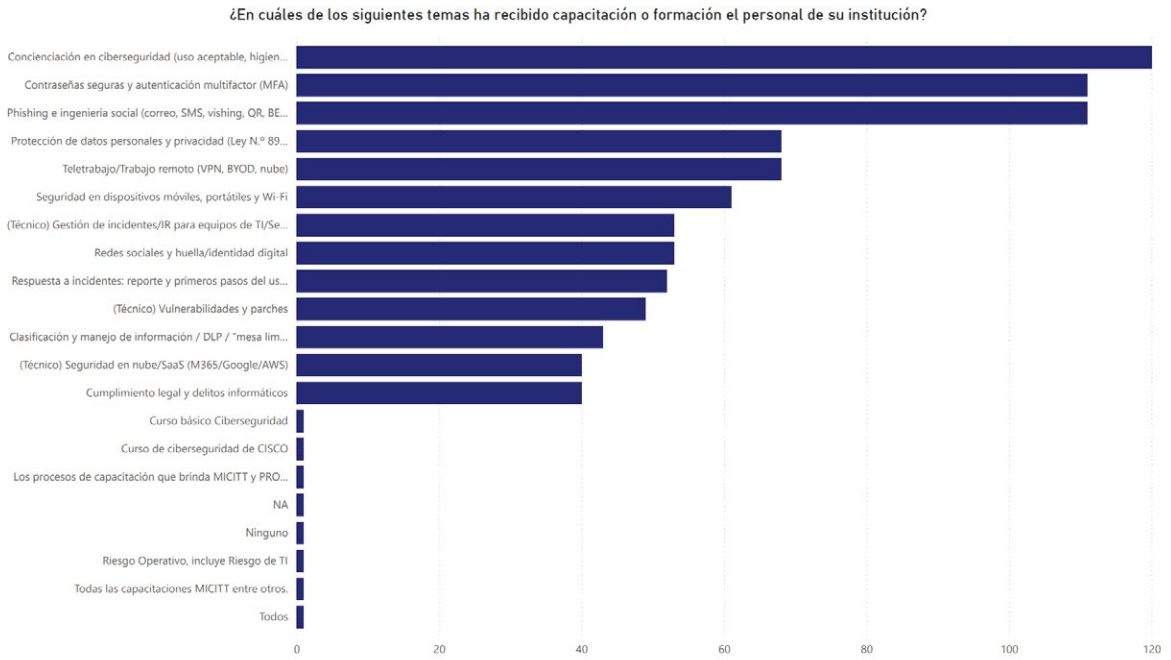
Gráfico 24. Participación/organización de conferencias o talleres sobre ciberseguridad



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

Asimismo, la mayoría de las instituciones indica que el personal ha recibido capacitación en temáticas básicas y transversales: concienciación en ciberseguridad (84,5 %), *phishing* e ingeniería social (78,2 %) y uso de contraseñas seguras y autenticación (78,2 %). A esto se suman, aunque en menor medida, contenidos como protección de datos personales, teletrabajo seguro, dispositivos móviles, redes sociales, gestión y respuesta a incidentes o cumplimiento legal. Aparecen menciones aisladas a «curso básico de ciberseguridad», «riesgo operativo», «procesos de capacitación internos» o incluso «ninguno», lo que refleja cierta disparidad en la profundidad de los programas. Pese a ello, un 59,2 % señala que la capacitación es obligatoria para todo el personal y otro grupo menor la exige solo para perfiles críticos; sin embargo, más de una quinta parte afirma que no es obligatoria, lo que sugiere una debilidad que puede disminuir la preparación del equipo humano en ciberseguridad.

Gráfico 25. Temáticas de formación y/o capacitación



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

Además, un 39,86 % de las instituciones encuestadas no ofrece a su personal programas de formación continua en línea (*e-learning*) en ciberseguridad, hallazgo que resalta limitaciones en el acceso a capacitación flexible y actualizada. Asimismo, existe disparidad en la disponibilidad de estos recursos: solo el 27,27 % de las instituciones los ofrece a todo el personal, y un 12,59 % los limita a equipos críticos, como TI o Seguridad.

En este contexto, los resultados sobre la disponibilidad de presupuesto para financiar certificaciones profesionales en ciberseguridad (exámenes, renovaciones y/o preparación) indican que un 34,97 % no cuenta con presupuesto y un 20,28 % no sabe o no responde, lo que refleja poca claridad interna sobre este tema. Solo un 14,69 % dispone de una línea presupuestaria específica y un 20,28 % lo gestiona caso por caso, mientras que un 9,9 % lo mantiene en evaluación. En conjunto, estos datos evidencian que el apoyo institucional para capacitar al personal mediante certificaciones continúa siendo limitado.

3.2.2.5. Procedimiento Legal

En el ámbito de los procedimientos legales, el nivel de familiaridad del personal con la normativa penal costarricense sobre delitos informáticos muestra una tendencia

clara: la mayor proporción de respuestas se concentra en quienes indican estar «algo familiarizadas» (36,36 %), seguida de un 20,4 % que afirma conocerla «poco» y un 20,28 % que señala estar «bastante familiarizada». Solo un 12,7 % indica tener un conocimiento profundo, mientras que un 9,09 % reconoce no estar familiarizada con esta normativa. Estos resultados evidencian que el conocimiento sobre este marco legal continúa siendo limitado, lo que refuerza la necesidad de fortalecer la formación institucional en materia jurídica relacionada con delitos informáticos.

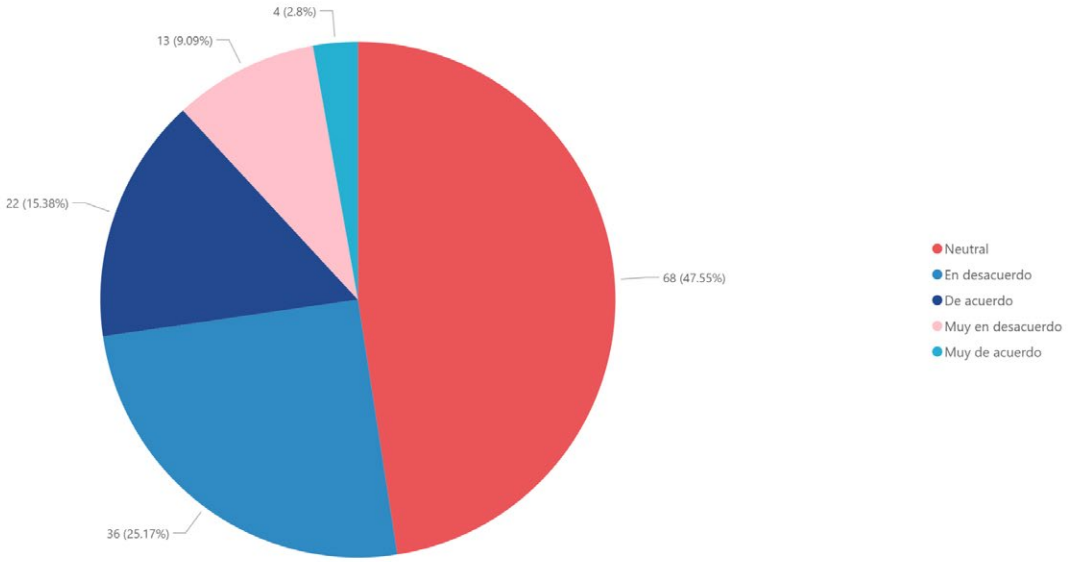
En relación con la adecuación de la normativa penal costarricense frente a los incidentes informáticos, las respuestas muestran una percepción marcada de insuficiencia. Aunque un 37,76 % considera que la ley es solo «parcialmente adecuada» y otro 37,76 % indicó no saber si realmente cubre los incidentes actuales, apenas un 9,79 % la percibe como adecuada y solo un 2,8 % como muy adecuada.

Los comentarios cualitativos revelan una percepción ampliamente compartida de que, aunque la normativa costarricense contempla delitos informáticos tradicionales como acceso indebido, sabotaje o estafa informática, su actualización sería insuficiente para enfrentar amenazas modernas. Además, señalan que el marco legal no acompaña la velocidad de la evolución tecnológica, dejando vacíos frente a incidentes como *ransomware*, técnicas avanzadas de suplantación, ataques transnacionales o el uso malintencionado de inteligencia artificial. Además, varias personas participantes consideran que la ley es demasiado general, poco técnica y carente de tipificaciones más específicas necesarias para abordar escenarios actuales.

Por otra parte, incluso quienes consideran que la normativa es aceptable destacan dificultades en su aplicación práctica, debido a limitaciones institucionales: escasos recursos investigativos, capacidades técnicas reducidas, problemas en la preservación de evidencia digital y desconocimiento de la normativa por parte de funcionarios clave. Esto genera una brecha entre lo que la ley podría abarcar y lo que efectivamente se logra judicializar. En conjunto, los comentarios reflejan la necesidad de reformas periódicas, fortalecimiento operativo y mayor divulgación, de modo que la normativa penal se conozca mejor y, además, se comprendan los marcos complementarios vinculados con la ciberdelincuencia internacional y el propio proceso penal costarricense.

Lo anterior se relaciona con la percepción sobre la efectividad de estas leyes y su capacidad para disuadir la ejecución de ciberdelitos. La mayoría adopta una posición neutral (47,55 %), mientras que un 25,17 % considera que las sanciones no son suficientemente efectivas. Solo un 15,38 % muestra algún nivel de acuerdo. En conjunto, los resultados sugieren que el marco sancionatorio actual no genera confianza plena como mecanismo disuasorio frente a la creciente cibercriminalidad.

Gráfico 26. Percepción sobre la efectividad y pertinencia de las sanciones legales por delitos informáticos



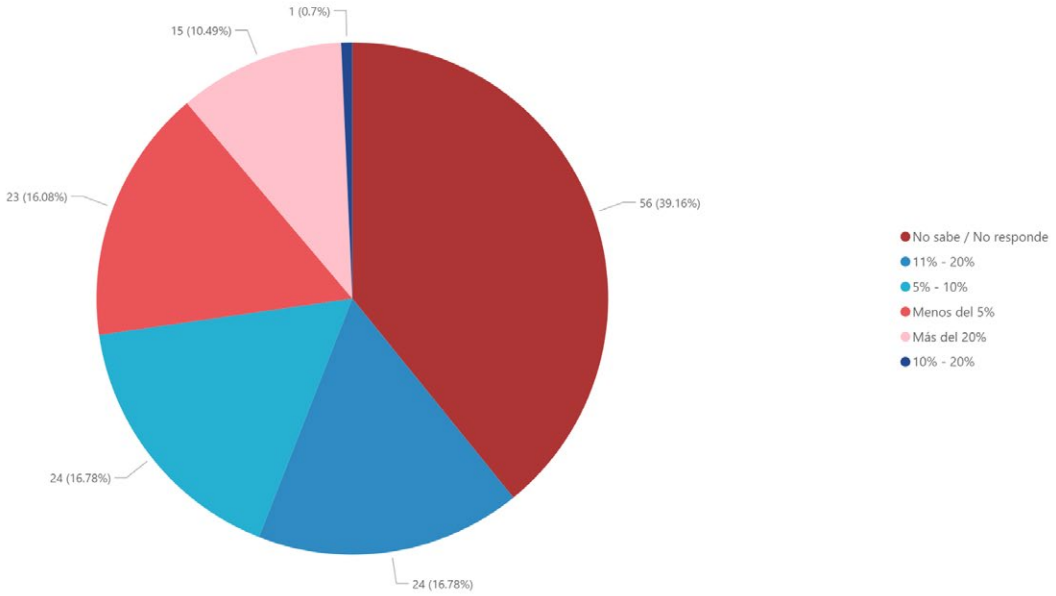
Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

3.2.2.6. Recursos y Presupuesto

Con el propósito de comprender el presupuesto y los recursos que las organizaciones destinan a la ciberseguridad, esta sección se enfoca en identificar las inversiones y capacidades disponibles para fortalecer su infraestructura tecnológica con base en las respuestas brindadas. La asignación de recursos en esta materia resulta fundamental, pues se traduce en estrategias más robustas, medidas preventivas, sistemas de detección y respuesta, así como en programas de formación y capacitación que permiten enfrentar adecuadamente las amenazas actuales.

Los resultados sobre la asignación presupuestaria en ciberseguridad muestran que esta continúa siendo limitada y poco visible dentro de las organizaciones, en línea con lo observado en ediciones anteriores. Aunque algunas personas participantes indican destinar menos del 10 % del presupuesto de TI a este rubro, la proporción más alta (39,16 %) afirma no conocer el monto asignado, lo que evidencia poca claridad o comunicación en la gestión financiera del área. Esta falta de definición se complementa con la percepción institucional: el 45,45 % considera que el presupuesto no es adecuado para cubrir sus necesidades de ciberseguridad, y solo un 24,48 % lo percibe suficiente. En este contexto, los datos sugieren que persisten brechas tanto en inversión como en planificación, lo que podría afectar la capacidad de las instituciones para responder a riesgos crecientes.

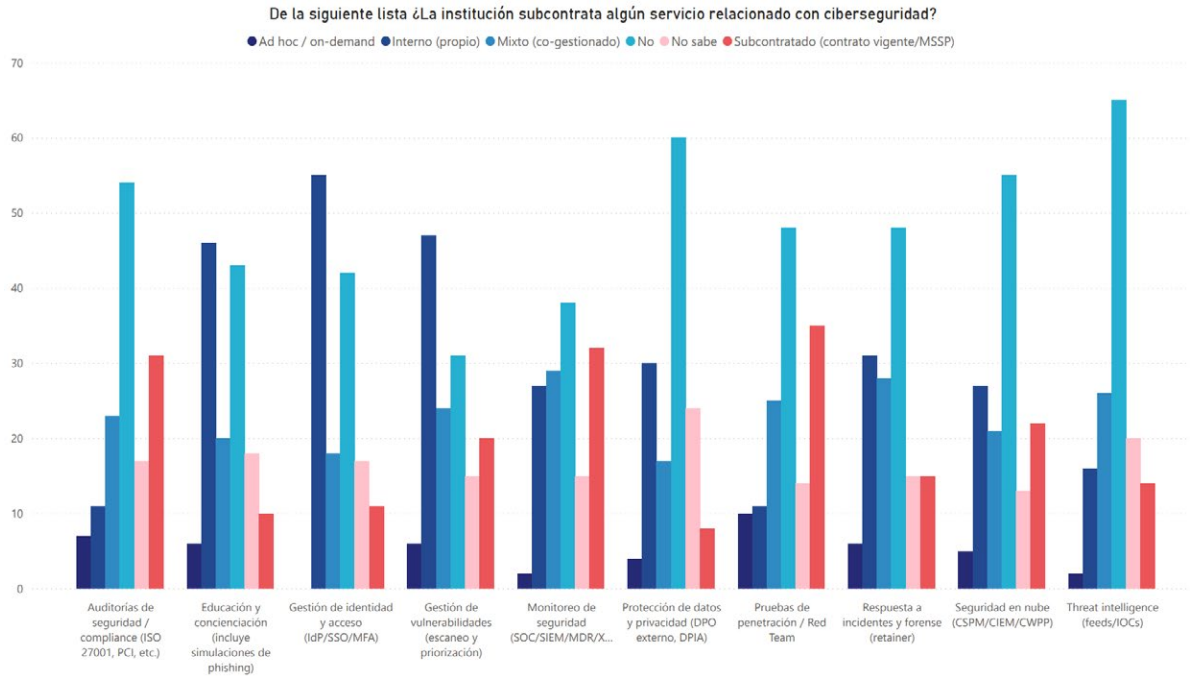
Gráfico 27. Asignación porcentual del presupuesto de TI destinado a ciberseguridad



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

De igual forma, al observar la subcontratación de servicios de ciberseguridad en 2025, se mantiene el patrón de que, en la mayoría de los rubros, las instituciones indican no contratar estos servicios de forma externa. Esta situación se aprecia especialmente en áreas especializadas como pruebas de penetración, auditorías de seguridad, inteligencia de amenazas, educación y concienciación, y protección de datos y privacidad, donde la barra de «No» domina claramente. Cuando sí se recurre a servicios externos, estos se concentran principalmente en monitoreo de seguridad (SOC/SIEM/MDR/XDR), respuesta a incidentes y gestión de vulnerabilidades, combinando esquemas internos, subcontratados y mixtos. En menor medida aparecen modelos *ad hoc/on-demand*, lo que sugiere que muchas organizaciones siguen dependiendo de capacidades internas limitadas y solo incorporan apoyo especializado externo en momentos puntuales, con posibles vacíos en servicios avanzados de ciberseguridad.

Gráfico 28. Subcontratación de Servicios relacionados con ciberseguridad

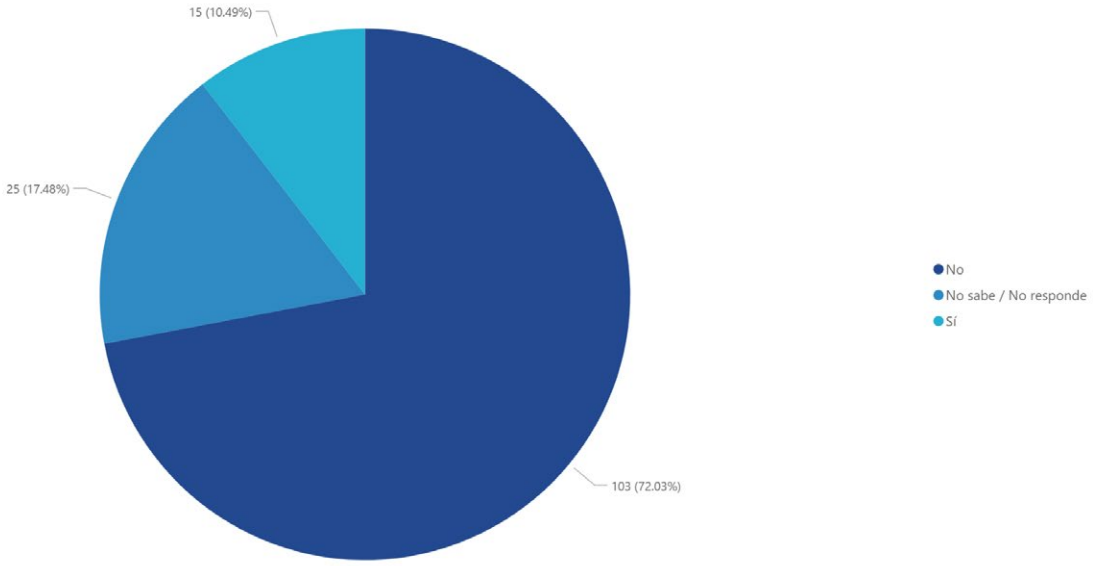


Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

3.2.2.7. Alcance Operativo

En el marco del alcance operativo, los resultados muestran que la gran mayoría de las instituciones encuestadas no desarrolla actividades en mercados internacionales (72,03 %), mientras que únicamente un 10,49 % sí opera fuera del país y un 17,48 % no tiene claridad al respecto. Entre las instituciones con presencia fuera del país, la operación se concentra principalmente en América del Norte (80 %) y América Central (73,3 %), seguidas de Europa (60 %) y América del Sur (53,3 %). En menor medida, reportan actividades en Asia (40 %) y en regiones como África, Medio Oriente y Oceanía (cada una con 13,3 %). Esto evidencia que, aunque el número de organizaciones con proyección internacional es reducido, quienes sí la tienen se mueven sobre todo en mercados del continente americano y europeo.

Gráfico 29. Evaluación de riesgos en mercados internacionales



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

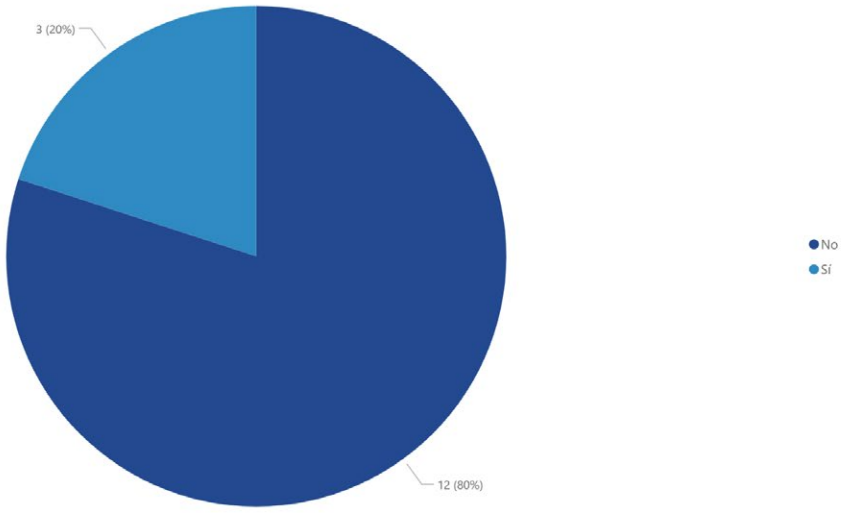
Los resultados muestran que, entre las organizaciones que operan en mercados internacionales, existe una diferencia marcada en cuanto a la gestión del riesgo. Aunque un 46,7 % indica que sí evalúa riesgos específicos para cada país donde opera, otra proporción equivalente señala no hacerlo o desconocerlo, lo cual evidencia falta de consistencia en las prácticas de gestión internacional. La adaptación de políticas internas sigue una tónica parecida. Aunque el 53,3 % alinea sus lineamientos de ciberseguridad con las normativas locales, el 33,3 % restante no realiza este proceso o no lo tiene claro, esta situación incrementa el riesgo de incumplimientos y exposición a sanciones.

En lo relativo a la protección de comunicaciones en contextos transfronterizos, las organizaciones reportan prácticas relativamente robustas. El 86,7 % indica utilizar VPN para acceso remoto y casi la mitad emplea, además, esquemas de VPN *site-to-site*. Esto se complementa con un 26,7 % que adopta soluciones más avanzadas, tales como arquitecturas de acceso de confianza cero (ZTNA) o servicios SASE. En conjunto, estos datos evidencian un enfoque de protección de las comunicaciones más alineado con estándares internacionales y con modelos contemporáneos de seguridad de redes.

Por otra parte, si bien cabría esperar una mayor exposición a incidentes al operar en múltiples jurisdicciones, el 80 % de las instituciones afirma no haber experimentado ataques en el exterior. Este resultado podría interpretarse, por un lado, como un

entorno internacional relativamente controlado; pero, por otro, también podría reflejar limitaciones en las capacidades de detección, registro o reporte de incidentes en dichos contextos.

Gráfico 30. Ataques cibernéticos en mercados extranjeros



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

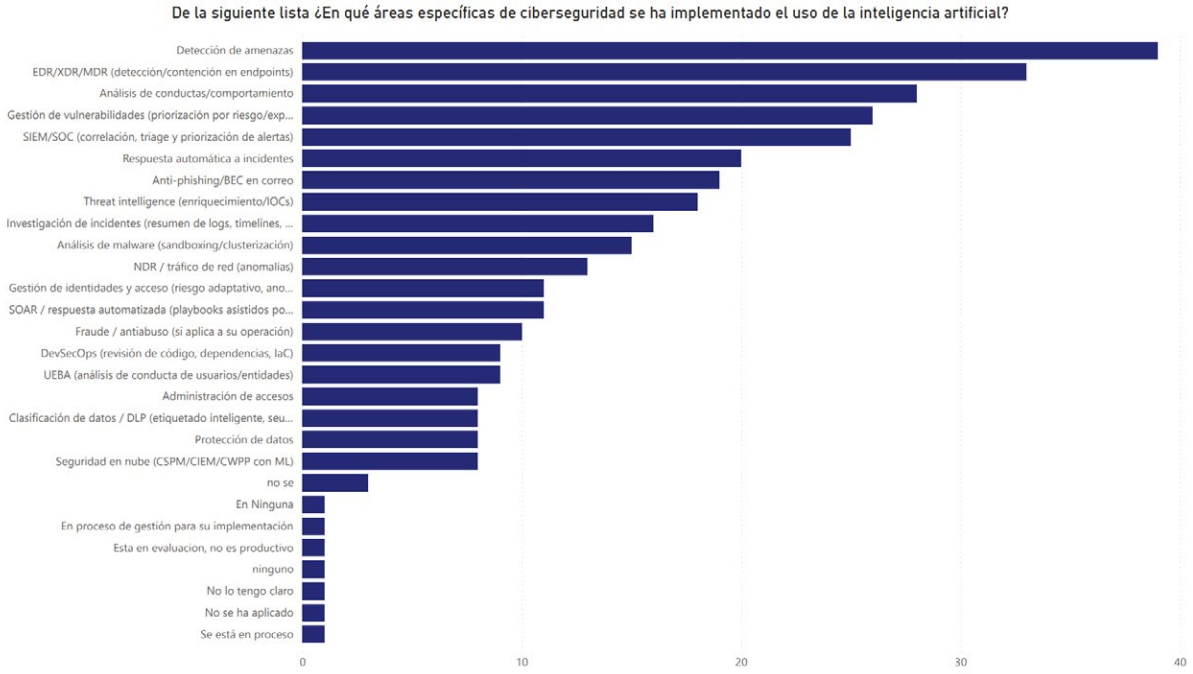
3.2.2.8. Inteligencia Artificial

En materia de adopción de inteligencia artificial (IA) aplicada a la ciberseguridad, los resultados evidencian que su incorporación aún es limitada. Solo un 12,59 % de las instituciones indica utilizarla en entornos de producción y un 7,69 % la mantiene en fase piloto, mientras que un 39,86 % no la emplea y un 20,98 % se encuentra en etapa de evaluación. A pesar de este nivel de adopción relativamente bajo, la percepción sobre su efectividad es mayoritariamente positiva entre quienes sí la han implementado: un 44,07 % la considera efectiva y un 20,34 % muy efectiva, en tanto que cerca de un tercio mantiene una postura neutral. En conjunto, estos datos sugieren que, aunque la IA todavía no forma parte integral de los procesos de ciberseguridad para la mayoría de las organizaciones, aquellas que ya la utilizan perciben beneficios claros, lo que apunta a un potencial de expansión futura conforme se consoliden las capacidades técnicas, los marcos de gobernanza y las inversiones asociadas a su despliegue.

En las áreas específicas donde se aplica la inteligencia artificial en ciberseguridad, los resultados muestran que su uso se concentra principalmente en las capas de monitoreo y detección. La mayoría de las instituciones que emplean IA la utilizan para detección de amenazas (67,2 %), seguida por EDR/XDR/MDR (56,9 %), herramientas

de detección y respuesta en *endpoints*, extendida y gestionada, y SIEM/SOC (43,1 %), plataformas de correlación de eventos y centros operativos de seguridad, donde los algoritmos apoyan la correlación de eventos y la priorización de alertas. A esto se suma un uso relevante en análisis de conductas o comportamiento (48,3 %), gestión de vulnerabilidades (44,8 %) y, en menor medida, respuesta automática a incidentes (34,5 %), *anti-phishing*/BEC (32,8%), análisis de *malware* (25,9 %) y NDR/tráfico de red (22,4 %), así como administración de accesos (12,1 %) e identidades. Finalmente, las respuestas aisladas como «ninguno», «no se ha aplicado» o «está en evaluación» evidencian que, si bien la IA comienza a integrarse de forma más sistemática en varios frentes técnicos, aún existe un grupo de organizaciones en fases exploratorias o sin un despliegue consolidado de estas capacidades.

Gráfico 31. Áreas específicas de ciberseguridad donde se ha implementado el uso de la inteligencia artificial

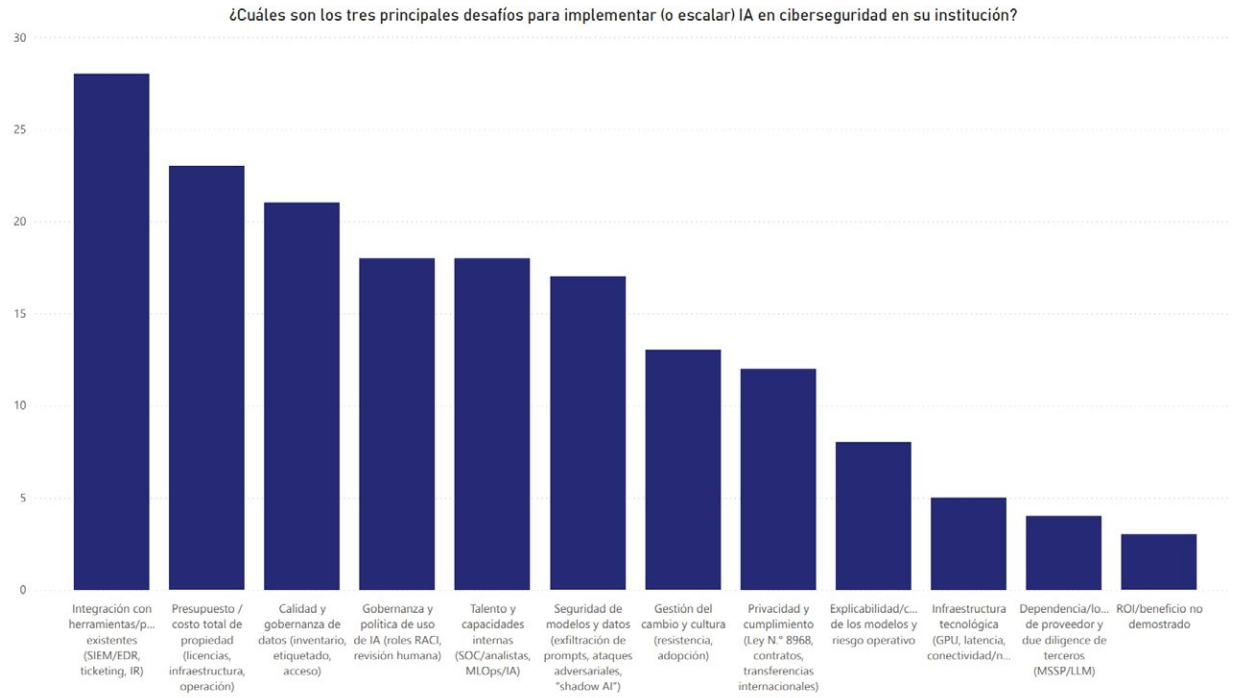


Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

En esta edición, los principales desafíos para implementar o escalar soluciones de inteligencia artificial en ciberseguridad presentan una distribución más diversificada que en 2024. Mientras que en la medición anterior la preocupación central se concentraba casi exclusivamente en la falta de personal especializado (100 %), en 2025 las personas encuestadas señalan como retos prioritarios la integración con las herramientas y plataformas existentes (46,6 %), los costos asociados a la implementación (39,7 %) y la calidad y gobernanza de los datos (36,2 %).

Adicionalmente, adquieren un peso creciente dimensiones como la seguridad de los modelos de IA (29,3 %) y la gobernanza de su uso (31 %), lo que sugiere que la discusión ha evolucionado desde un enfoque centrado primordialmente en la disponibilidad de talento hacia un abordaje más amplio de desafíos técnicos, organizacionales y de gobierno de la tecnología.

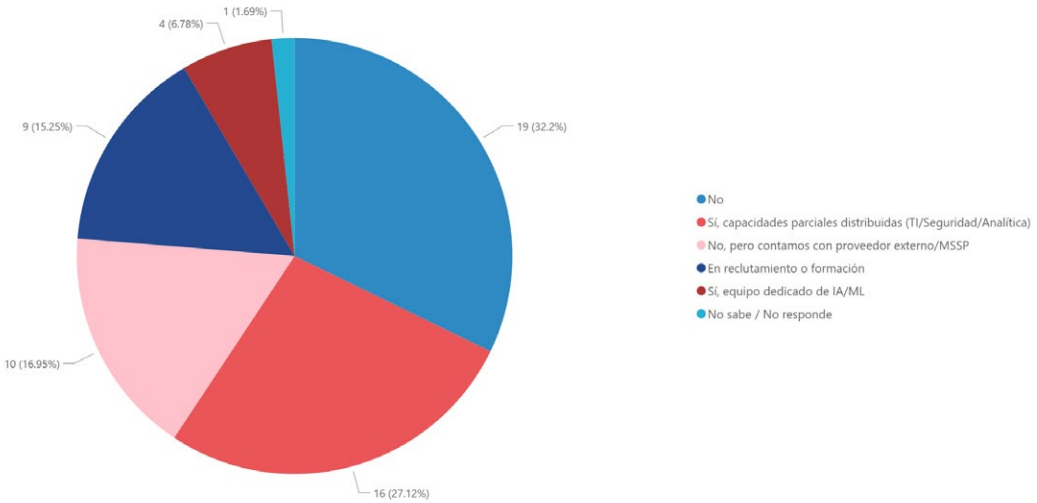
Gráfico 32. Desafíos en la implementación de IA en ciberseguridad



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

Específicamente sobre el componente de personal calificado para IA, los resultados de 2025 reflejan una visión distinta a la edición anterior. Aunque persiste la limitación, ya no representa el consenso absoluto de 2024. Un 6,78 % reporta contar con un equipo dedicado, un 27,12 % dispone de capacidades parciales distribuidas entre TI/Seguridad y un 32,2 % no cuenta con personal calificado. Además, un 16,95 % depende de proveedores externos y otro 15,25 % se encuentra en procesos de reclutamiento o formación. Si bien la escasez de talento continúa siendo un factor relevante, los datos de 2025 indican que no es el único eje crítico, a diferencia de 2024, donde sí lo fue.

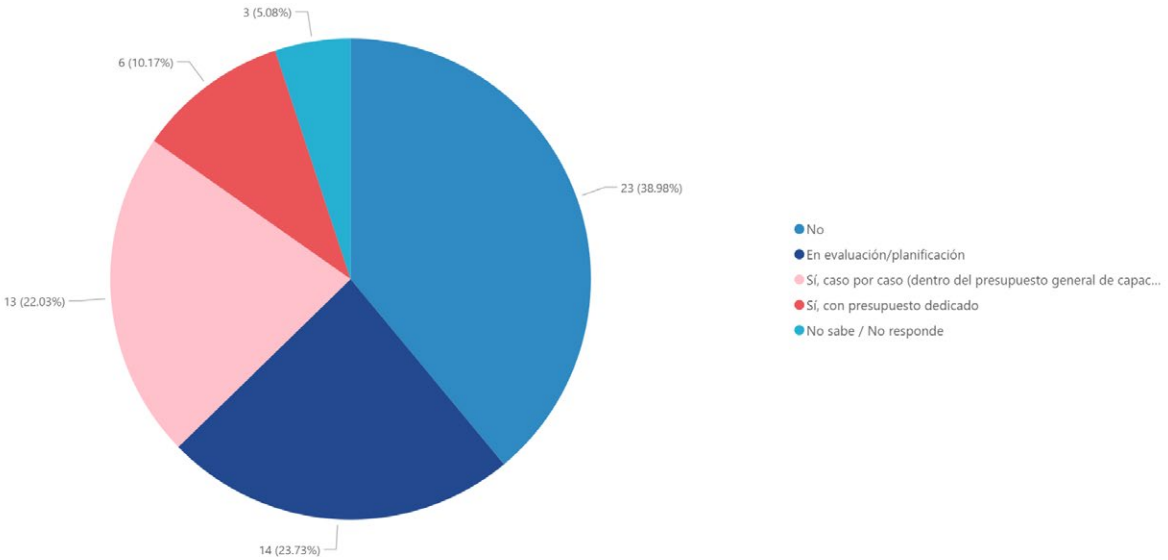
Gráfico 33. Personal capacitado en IA



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

En cuanto a formación en IA, los resultados confirman un desafío persistente: el 38,98 % no invierte actualmente en capacitación en IA aplicada a la ciberseguridad, cifra incluso superior a la registrada en 2024 (37,5 %). Solo un 10,17 % asigna presupuesto dedicado y un 22,03 % lo hace de manera puntual. Esto refleja que, pese a reconocer nuevos desafíos técnicos y de gobernanza, la inversión interna para desarrollar capacidades sigue siendo limitada, lo que dificulta que las organizaciones avancen hacia una adopción más sólida de tecnologías basadas en IA.

Gráfico 34. Inversión en formación y capacitación en inteligencia artificial (IA) aplicada a la ciberseguridad



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

Conclusiones

UNA UNIVERSIDAD NACIONAL COSTA RICA

LABORATORIO DE I+D+i LABCIBE EN CIBERSEGURIDAD

VICERRECTORÍA DE INVESTIGACIÓN UNIVERSIDAD NACIONAL

WWW.UNA.AC.CR

Reflexiones finales sobre los resultados de la encuesta 2025

El diagnóstico derivado de la encuesta 2025 muestra que la ciberseguridad en Costa Rica se consolida progresivamente como un componente estructural de la gestión institucional, aunque aún presenta importantes asimetrías y brechas de madurez entre sectores. En contraste con las ediciones 2023 y 2024, el aumento del número de respuestas y la mayor diversidad de instituciones participantes fortalecen la capacidad descriptiva del estudio y consolidan la serie como un instrumento útil para la observación de tendencias. Se confirma, además, que la ciberseguridad ha dejado de ser un asunto exclusivamente técnico: en los tres años analizados se aprecia una incorporación paulatina del tema en las agendas de gobernanza, cumplimiento y gestión de riesgos, con una presencia cada vez más visible de políticas internas, manuales de respuesta a incidentes y acciones de sensibilización dirigidas al personal. Si bien estas capacidades ya se vislumbraban en 2023, en 2024 y 2025 tienden a estabilizarse e incluso a ampliarse, particularmente en sectores regulados, como el financiero y el público.

No obstante, la lectura integrada de los tres ciclos (2023, 2024 y 2025) revela que dicha institucionalización convive con déficits estructurales difíciles de soslayar. La reducción sostenida de la oferta formativa formal en ciberseguridad, que pasa de niveles altos en 2023 a cifras intermedias en 2024 y se ubica en 2025 en una proporción claramente minoritaria, así como la limitada visibilidad de iniciativas de investigación y desarrollo, apuntan a una fragilidad persistente en el ecosistema de conocimiento. En 2023 el énfasis estaba puesto en la consolidación de programas y líneas de trabajo incipientes; en 2024 ya se advertían señales de desaceleración; en 2025 la tendencia descendente se hace más evidente. De mantenerse esta trayectoria, la capacidad del país para generar soluciones propias, innovar y responder a amenazas emergentes podría verse comprometida, trasladando el peso de la respuesta hacia la contratación de servicios externos y reduciendo el margen de autonomía tecnológica.

De forma paralela, la opacidad presupuestaria se muestra como una constante a lo largo de las tres ediciones. Desde 2023, una proporción relevante de personas encuestadas declara no conocer el porcentaje de recursos de TI asignados a ciberseguridad ni la existencia de presupuestos específicos para I+D. Esta pauta se repite en 2024 y vuelve a aparecer en 2025, en algunos casos incluso con mayor peso relativo que en años anteriores. Ello sugiere que, aunque existen esfuerzos puntuales de inversión y proyectos relevantes en ciertas instituciones, estos no siempre se articulan a una planificación estratégica clara ni a una gestión basada en evidencia. En términos de política pública, la estabilidad de la categoría «no sabe/no responde»

indica que el problema no es únicamente de falta de recursos, sino también de gobernanza financiera: la ciberseguridad continúa siendo, en muchos casos, un componente difuso del presupuesto institucional y no una línea de inversión explícita y trazable.

Las brechas en gestión de riesgos, protección de datos personales y cultura de reporte de incidentes refuerzan esta lectura longitudinal. Entre 2023 y 2025 se observan avances graduales en la existencia de instrumentos normativos y en la adopción de determinadas medidas técnicas; sin embargo, la proporción de instituciones que no realiza evaluaciones formales de riesgo, que mantiene controles parciales sobre datos personales o que no canaliza incidentes hacia el sistema de justicia se mantiene en rangos preocupantes. Es decir, la tendencia muestra mejoras incrementales en lo declarativo (políticas, reglamentos, protocolos) y en ciertos controles específicos, pero sin que ello se traduzca en un cierre robusto del ciclo de gestión del riesgo. A lo largo de los tres años, los resultados evidencian dificultades para completar de manera sistemática y verificable las etapas de identificación, evaluación, tratamiento, monitoreo y comunicación de los riesgos de ciberseguridad.

En este contexto, la evolución de la temática de inteligencia artificial aplicada a la ciberseguridad introduce un elemento diferenciador en la serie 2023–2025. En la primera edición, la IA aparecía de manera residual o conceptual; en 2024 emergía como un ámbito de interés estratégico, aunque con pocas implementaciones concretas; en 2025 se constata la existencia de experiencias incipientes, pero operativas, en detección de amenazas, monitoreo de eventos, análisis de comportamiento y gestión de vulnerabilidades. Los datos muestran que, entre 2024 y 2025, crece tanto la proporción de instituciones que exploran pilotos como la de aquellas que la incorporan en producción, y que la valoración de su efectividad es mayoritariamente positiva. Sin embargo, la misma serie temporal pone en evidencia que este desarrollo se ve sistemáticamente limitado por factores que se repiten año con año: escasez de talento especializado, dependencia de proveedores externos, ausencia de esquemas robustos de gobernanza y capacitación, y falta de presupuestos específicos. La IA se perfila, así, como un vector dual: por un lado, una herramienta con capacidad para incrementar de manera significativa la eficacia de la defensa; por otro, un posible amplificador de brechas si su adopción queda restringida a pocas instituciones con mayores capacidades tecnológicas y financieras.

Desde el conjunto de respuestas analizadas sugiere que el comportamiento de los indicadores a lo largo de las tres ediciones invita a interpretar la ciberseguridad no solo como un conjunto de prácticas técnicas, sino como una política pública transversal que requiere coherencia entre marcos jurídicos, estructuras de gobernanza, capacidades institucionales, formación de talento y asignación de recursos. Los resultados de 2023 ya señalaban debilidades en la actualización normativa y en la articulación entre

actores; en 2024 se consolidó la percepción de desajuste entre la velocidad de las amenazas y el ritmo de reforma legal; en 2025 se mantiene e incluso se profundiza la demanda por marcos regulatorios más específicos, operativos y alineados con estándares internacionales. A nivel de gobernanza, la serie completa pone de relieve la necesidad de contar con lineamientos nacionales claros, mecanismos efectivos de coordinación interinstitucional y esquemas de supervisión y rendición de cuentas que permitan traducir principios generales en obligaciones concretas y medibles.

En suma, los resultados de la encuesta 2025, leídos a la luz de las ediciones 2023 y 2024, ofrecen una fotografía compleja y dinámica. Por un lado, muestran avances innegables en términos de sensibilización, formalización de políticas internas y desarrollo de capacidades básicas, con una trayectoria que, aunque desigual, es claramente ascendente en varios indicadores clave. Por otro, evidencian la persistencia, y en algunos casos la profundización, de brechas entre la retórica sobre la importancia de la ciberseguridad y la consistencia de las inversiones, estructuras y procesos necesarios para sostenerla en el tiempo. En la medida en que este estudio se consolida como un ejercicio periódico de medición, sus hallazgos deben ser leídos no solo como un diagnóstico coyuntural, sino como una hoja de ruta de mediano plazo que oriente la toma de decisiones de actores públicos, privados y académicos. Fortalecer la oferta formativa y la investigación, dotar de mayor transparencia y previsibilidad a los recursos invertidos, cerrar brechas en protección de datos y gestión de riesgos, y articular la estrategia nacional para el uso responsable de la inteligencia artificial en ciberseguridad emergen, así, como líneas prioritarias de acción para el próximo ciclo de políticas, programas y reformas en la materia. En conjunto, los hallazgos del *Estado de la Ciberseguridad 2025* refuerzan la necesidad de consolidar la ciberseguridad como una política pública transversal, sostenida y basada en evidencia, capaz de articular capacidades normativas, institucionales, humanas y tecnológicas frente a un entorno de riesgo creciente y dinámico.

De cara a futuras ediciones, los resultados obtenidos entre 2023 y 2025 permiten sentar las bases para el fortalecimiento progresivo de un enfoque longitudinal híbrido, combinando levantamientos anuales comparables con la eventual incorporación de un panel institucional parcial. Este enfoque permitiría mejorar la comparabilidad interanual, profundizar el análisis por sectores estratégicos y robustecer la utilidad del informe como insumo para la formulación y evaluación de políticas públicas en ciberseguridad.

Referencias bibliográficas

Artavia León, J., & Soto Sotelo, M. (2023). *Evaluación del sistema de gestión de resiliencia y de ciberseguridad en un proveedor de internet* [Trabajo final de graduación, Universidad Cenfotec].

Asamblea Legislativa de la República de Costa Rica. (2001, 16 de octubre). *Ley de la Administración Financiera de la República y Presupuestos Públicos*.

Asamblea Legislativa de la República de Costa Rica. (2001, 24 de octubre). *Adición de los artículos 196 bis, 217 bis y 229 bis al Código Penal*.

Asamblea Legislativa de la República de Costa Rica. (2005, 13 de octubre). *Ley de Certificados, Firmas Digitales y Documentos Electrónicos (Ley N.° 8454)*. https://pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=55666

Asamblea Legislativa de la República de Costa Rica. (2008). *Tratado de Libre Comercio República Dominicana–Centroamérica–Estados Unidos (DR-CAFTA)*, Capítulo 13. https://www.comex.go.cr/tratados/cafta-dr/texto-del-tratado-1/

Asamblea Legislativa de la República de Costa Rica. (2011, 5 de septiembre). *Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales (Ley N.° 8968)*. https://pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975

Asamblea Legislativa de la República de Costa Rica. (2011, 8 de septiembre). *Ley de protección de la niñez y la adolescencia frente al contenido nocivo de internet y otros medios electrónicos*.

Asamblea Legislativa de la República de Costa Rica. (2012). *Reforma de varios artículos y modificación de la Sección VIII «Delitos informáticos y conexos» del Título VII del Código Penal (Ley N.° 9048)*.

Asamblea Legislativa de la República de Costa Rica. (2019). *Ley para Regular el Teletrabajo (Ley N.° 9738)*.

Asamblea Legislativa de la República de Costa Rica. (2024). *Ley Marco de Acceso a la Información Pública (Ley N.° 10554)*. https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=103157&nValor3=143061&strTipM=TC

Banco Central de Costa Rica. (2011). Banco Central de Costa Rica (sitio institucional). http://www.bccr.fi.cr/sobre_bccr/

Barrantes Sliesarieva, E. G. (2010). *Conceptualización de la ciberseguridad*. PROSIC–UCR.

Cámara de Tecnologías de Información y Comunicación (CAMTIC). (s. f.). Acerca de CAMTIC. https://www.camtic.org/quienes-somos

Comisión de Currículo Universitario. (2022). *Lineamientos para la creación y rediseño de carreras universitarias estatales*. https://repositorio.conare.ac.cr/handle/20.500.12337/8455

Comisión Europea. (2012). *Proposal on a European Strategy for Internet Security*. http://ec.europa.eu/governance/impact/planned_ia/docs/2012_infso_003_european_internet_security_strategy_en.pdf

Comunidad Europea. (1992, julio). *Tratado de Maastricht*. Banco Central Europeo. http://www.ecb.int/ecb/legal/pdf/maastricht_en.pdf

Comisión Nacional de Supervisión del Sistema Financiero (CONASSIF). (2024, 5 de agosto). *Acuerdo CONASSIF 5-24: Reglamento General de Gobierno y Gestión de la Tecnología de la Información* (v01). https://www.sugef.fi.cr/normativa/normativa_transversal/documentos/CONASSIF%205-24%20(v01%205%20agosto%202024).pdf

Consejo de Europa. (2001, 23 de noviembre). *Convention on Cybercrime (Budapest)*. http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

Consejo Nacional de Enseñanza Superior Universitaria Privada (CONESUP). (2021). *Procedimientos 2020–2021*. https://conesup.mep.go.cr/sites/all/files/procedimientos_2020-2021_version_0.4.pdf

Consejo Nacional de Enseñanza Superior Universitaria Privada (CONESUP). (s. f.). Inicio. https://conesup.mep.go.cr/

Consejo Nacional de Rectores (CONARE). (s. f.). Inicio. https://www.conare.ac.cr/

Costa Rica, Poder Ejecutivo. (2017). *Apertura de Datos Públicos (Decreto Ejecutivo N.º 40199-MP)*. https://pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=5027

Costa Rica, Poder Ejecutivo. (2024). *Reglamento para la gobernanza en ciberseguridad y la resiliencia cibernética de las instituciones gubernamentales* (Decreto Ejecutivo N.º 45061-MICITT). https://pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=104718

Costa Rica, Poder Ejecutivo (Hacienda–MICITT). (s. f.). *Privilegiar la adquisición de soluciones de cómputo en la nube sobre otro tipo de infraestructura (Directriz N.º 46-H-MICITT)*. https://pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=74850

Costa Rica, Poder Ejecutivo (Hacienda–MICITT). (s. f.). *Regulación y normalización de adquisiciones de tecnología y/o desarrollo de sistemas informáticos de apoyo a la gestión (Directriz N.º 053-H-MICITT)*. (Base PGR).

Costa Rica, Poder Ejecutivo (JP). (2013). *Reglamento a la Ley N.º 8968 (Decreto Ejecutivo N.º 37554-JP)*. https://pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=74352

Costa Rica, Poder Ejecutivo (MICITT). (2023). *Lineamientos para la implementación del proyecto de fortalecimiento de las capacidades en ciberseguridad del país (Decreto Ejecutivo N.º 44487-MICITT)*. http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=102171&nValor3=141134

Costa Rica, Poder Ejecutivo (MP–MICITT). (2023). *Directriz N.º 133: Marca de hora*. https://www.micitt.go.cr/sites/default/files/2023-06/DIRECTRIZ-N%C2%B0-133-marca-de-hora.pdf

Costa Rica, Poder Ejecutivo (MSP–MICITT). (2023). *Reglamento sobre medidas de ciberseguridad aplicables a los servicios de telecomunicaciones basados en la tecnología 5G y superiores (Decreto Ejecutivo N.º 44196-MSP-MICITT)*. https://pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=100155

Costa Rica, Poder Ejecutivo (MTSS–MICITT). (2023). *Implementación de accesibilidad de la red de los sitios del sector público (Directriz N.º 036-MTSS-MICITT)*. https://pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=101480

CRHoy. (2025, 5 de marzo). Abren maestría en ciberseguridad industrial en la UNA de Guanacaste. https://crhoy.com/tecnologia/abren-maestria-en-ciberseguridad-industrial-en-la-una-de-guanacaste/

CRHoy.com. (s. f.). Sede Chorotega de la UNA aprueba crear Maestría en Ciberseguridad Industrial. https://www.crhoy.com/tecnologia/sede-chorotega-de-la-una-aprueba-crear-maestria-en-ciberseguridad-industrial/

CyberSec Cluster. (s. f.). CyberSec Cluster. https://www.cybersec.cr/

Dirección Firma Digital. (s. f.). Firma digital (portal informativo). http://www.firmadigital.go.cr/Info.html

Fischer, E. A. (2012, 29 de junio). Federal laws relating to cybersecurity: Discussion of proposed revisions (CRS Report). https://www.fas.org/sgp/crs/natsec/R42114.pdf

Gobierno Digital – Secretaría Técnica. (s. f.). Gobierno Digital. http://www.gobiernofacil.go.cr/e-gob/gobiernodigital/index.html

Grupo de los Ocho (G8). (2010, junio). *Muskoka Declaration*. Ministerio de Relaciones Exteriores de Japón. http://www.mofa.go.jp/policy/economy/summit/2010/pdfs/declaration_1006.pdf

Grupo de los Ocho (G8). (2011, 26 de mayo). *Deauville Declaration: Internet*. http://www.g7.utoronto.ca/summit/2011deauville/2011-internet-en.html

Instituto Tecnológico de Costa Rica (TEC). (2022). Maestría en Investigación Empresarial. https://www.tec.ac.cr/carreras/maestria-investigacion-empresarial

Instituto Tecnológico de Costa Rica (TEC). (2022). *Automatización, ciberseguridad y ciencia de datos: nueva estrategia empresarial* [Recurso institucional].

International Telecommunication Union (ITU). (2006). *Resolution 130*. http://www.itu.int/osg/csd/intgov/mandate/Res130.pdf

International Telecommunication Union (ITU). (2007). *Global Cybersecurity Agenda (GCA) – Goals*. http://www.itu.int/osg/csd/cybersecurity/gca/goals.html

International Telecommunication Union (ITU). (2007). *International Cybersecurity Agenda* (GCA): Framework for international cooperation in cybersecurity. www.ifap.ru/library/book169.pdf

International Telecommunication Union (ITU). (2008). *GCA High-Level Experts' Group (HLEG) Global Strategy Report*. http://www.cybersecurity-gateway.org/pdf/global_strategic_report.pdf

International Telecommunication Union (ITU). (2008). *Resolution 45 – Encourage the creation of national computer incident response teams*. http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.58-2008-PDF-E.pdf

International Telecommunication Union (ITU). (2008). *Resolution 50 – Cybersecurity*. http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2008-PDF-E.pdf

International Telecommunication Union (ITU). (2008). *Resolution 52 – Countering and combating spam*. http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.52-2008-PDF-E.pdf

International Telecommunication Union (ITU). (2009). *Toolkit for cybercrime legislation*. http://www.cyberdialogue.ca/wp-content/uploads/2011/03/ITU-Toolkit-for-Cybercrime-Legislation.pdf

International Telecommunication Union (ITU). (2010). *Resolution 130*. http://www.itu.int/ITU-D/cyb/cybersecurity/WSIS/RESOLUTION_130.pdf

International Telecommunication Union (ITU). (2010). *Resolution 179*. http://www.itu.int/osg/csd/cybersecurity/gca/cop/RESOLUTION_179.pdf

International Telecommunication Union (ITU). (2010). *Resolution 181*. http://www.itu.int/osg/csd/cybersecurity/WSIS/RESOLUTION_181.pdf

International Telecommunication Union (ITU). (2010). *WSIS Resolution 45*. http://www.itu.int/osg/csd/cybersecurity/WSIS/RESOLUTION_45.pdf

International Telecommunication Union (ITU). (2010). *Resolution 69 – Creation of national CIRTs and cooperation*. http://www.itu.int/osg/csd/intgov/resoultions_2010/resolution69.pdf

ISACA. (2021). ISACA glossary. https://www.isaca.org/resources/glossary

Joyanes Aguilar, L. (2006). *Cibersociedad: Los retos sociales ante un nuevo mundo digital*. McGraw-Hill.

LabCIBE–UNA. (2025). *Estado de la ciberseguridad en Costa Rica 2024*. Universidad Nacional.

Lead University. (s. f.). Técnico Especializado en Ciberseguridad. https://ulead.ac.cr/es/carreras/programas-la-medida-y-especialidades/especialidad-en-ciberseguridad

Lemaitre Picado, R. (2011). *Manual sobre delitos informáticos para la ciber-sociedad costarricense*. Investigaciones Jurídicas S. A.

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT). (2023). E*strategia de Transformación Digital 2023–2027*. https://www.micitt.go.cr/sites/default/files/GobernanzaDigital/ETD%202023-2027%20V%20FINAL%2030-08-2023_v2.pdf

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT). (2023). *Estrategia Nacional de Ciberseguridad 2023–2027*. https://www.micitt.go.cr/sites/default/files/2023-11/NCS%20Costa%20Rica%20-%2010Nov2023%20SPA.pdf

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT). (2024). *Estrategia Nacional de Inteligencia Artificial 2024–2027*. https://www.micitt.go.cr/sites/default/files/2024-10/Estrategia%20Nacional%20de%20Inteligencia%20Artificial%20de%20Costa%20Rica%20ESP.pdf

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT). (2024). *Oficialización del Código Nacional de Tecnologías Digitales (Decreto Ejecutivo N.º 44507-MICITT)*. http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=102229&nValor3=0

Ministerio de Ciencia y Tecnología (MICIT). (s. f.). Firma digital (documentación técnica DCFD). http://www.firmadigital.go.cr/DCFD.html

Ministerio de Ciencia y Tecnología (MICITT). (2023, 12 de diciembre). Indicadores nacionales de ciencia, tecnología e innovación 2022 [presentación]. https://www.micitt.go.cr/sites/default/files/2023-12/Presentaci%C3%B3n%20Indicadores_2022%20-%2012%20diciembre%202023.pdf

Ministerio de Educación Pública (MEP). (2020). Programa de Técnico en Ciberseguridad. https://www.mep.go.cr/sites/default/files/programadeestudio/programas/ciberseguridad-X.pdf

Ministerio de Promoción de la Innovación y la Investigación (PROMOTORA). (2023). *Análisis de los desafíos 2023: Sector ciencia, tecnología, innovación y telecomunicaciones (DOCPLAN-03601)*. https://www.promotora.go.cr/web/Assets/pdfs/DOCPLAN-03601.pdf

OEA – Organización de los Estados Americanos. (2003). *Declaración sobre Seguridad en las Américas*. http://www.oas.org/csh/CES/documentos/ce00339s02.doc

OEA – Organización de los Estados Americanos. (2004, 8 de Junio). *Adoption of a comprehensive Inter-American strategy to combat threats to cybersecurity*. http://www.oas.org/XXXIVGA/english/docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm

Oficina Ejecutiva del Presidente de los Estados Unidos. (2000). *National plan for information systems protection. Federación de Científicos Americanos*. http://www.fas.org/irp/offdocs/pdd/CIP-plan.pdf

Oficina Ejecutiva del Presidente de los Estados Unidos. (2011, 16 de mayo). *International strategy for cyberspace: Prosperity, security, and openness in a networked world*. Casa Blanca. http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

Organismo de Investigación Judicial (OIJ), Unidad de Análisis Criminal. (2025). Estadísticas de delitos informáticos 2018–2025 (corte 31/08/2025): Respuesta a solicitud 2504-OPO/UAC/S-2025. San José, Costa Rica.

Organización de las Naciones Unidas (ONU). (2002, 23 de enero). *Resolution A/RES/56/121*. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf

Organización de las Naciones Unidas (ONU). (2002, 20 de diciembre). *Resolution A/RES/57/239*. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf

Organización de las Naciones Unidas (ONU). (2004, 30 de enero). *Resolution A/RES/58/199*. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N03/506/52/PDF/N0350652.pdf

Organización de las Naciones Unidas (ONU). (2011, 2 de diciembre). *Developments in the field of information and telecommunications in the context of international security*. http://www.un.org/disarmament/HomePage/ODAPublications/DisarmamentStudySeries/PDF/DSS_33.pdf

Poder Ejecutivo & Ministerio de Justicia y Gracia. (2002, 21 de febrero). *Directrices relativas al empleo ilegal de software en oficinas gubernamentales y autorización para empleo de software libre*. http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=47957&nValor3=92050&strTipM=TC

Poder Ejecutivo, Ministerio de Ciencia y Tecnología. (2004, 6 de mayo). *Reglamento de Control y Regulación de Locales que ofrecen Servicio Público de Internet*. http://historico.gaceta.go.cr/pub/2004/05/06/COMP_06_05_2004.pdf

Poder Ejecutivo, Ministerio de Ciencia y Tecnología. (2005, 23 de junio). Sobre el establecimiento de sitios web en las entidades públicas. http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=89061&nValor3=116705&strTipM=TC

Poder Ejecutivo, Ministerio de Ciencia y Tecnología. (2010, 9 de diciembre). *Creación de la Comisión Nacional de Seguridad en Línea*. http://historico.gaceta.go.cr/pub/2010/12/09/COMP_09_12_2010.pdf

Poder Ejecutivo, Ministerio de Ciencia y Tecnología. (2012, 13 de abril). *Creación del Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR)*.

Poder Ejecutivo, Ministro de la Presidencia y Ministra de Planificación. (2010, 4 de octubre). *Reforma al artículo 1.º del Decreto Ejecutivo N.º 35139-MP-MIDEPLAN que crea la Comisión Intersectorial de Gobierno Digital*.

Poder Ejecutivo, Ministros de la Presidencia y de Planificación. (2009, 6 de abril). *Créase la Comisión Interinstitucional de Gobierno Digital*.

Repositorio Instituto Tecnológico de Costa Rica (TEC). (s. f.). Repositorio TEC. https://repositoriotec.tec.ac.cr

Repositorio Universidad Cenfotec. (s. f.). Librarika. https://ucenfotec.librarika.com/search

Repositorio Universidad Nacional (UNA). (s. f.). SIDUNA. https://www.siduna.una.ac.cr/index.php

Repositorio Universidad Latina de Costa Rica. (s. f.). Repositorio institucional. https://repositorio.ulatina.ac.cr

Salas Ruiz, J. F. (2010). El Convenio de Europa sobre ciberdelincuencia. En PROSIC, Ciberseguridad en Costa Rica. Këwá–UCR. http://www.kerwa.ucr.ac.cr/bitstream/handle/10669/500/libro%20completo%20Ciber.pdf

Sincyt – Sistema Nacional de Ciencia, Tecnología e Innovación. (s. f.). I*ndicadores nacionales de CTI: Indicador 7*. https://sincyt.go.cr/Indicadores/indicadores/indicador7.jsf

Sincyt – Sistema Nacional de Ciencia, Tecnología e Innovación. (s. f.). Panel de indicadores CTI. https://sincyt.go.cr/Indicadores/home/dash-indicadores.jsf

Superintendencia General de Entidades Financieras (SUGEF). (2024, 29 de mayo). *SUGEF 10-07: Reglamento sobre divulgación de información y publicidad de productos y servicios financieros (v4)*. https://www.sugef.fi.cr/ver/normativa/normativa_vigente/SUGEF%2010-07%20(v4%2029%20mayo%202024).pdf#InformacionFicha

Superintendencia de Telecomunicaciones (SUTEL). (2011). Qué es y funciones de la SUTEL [Página institucional]. http://sutel.go.cr/Ver/Contenido/que-es-y-funciones-de-la-sutel/41

Superintendencia de Telecomunicaciones (SUTEL). (2022). *Reglamento sobre el régimen de protección al usuario final (RPUF) (Resolución RE-0062-JD-2022)*. https://pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=97801

Unión Internacional de Telecomunicaciones (UIT). (s. f.). ITU News (ed. 2010/09). http://www.itu.int/net/itunews/issues/2010/09/20-es.aspx

Universidad Cenfotec. (2024). *Propuesta de mejora ágil en el sistema software gestor de certificados digitales Enterprise para Intel* [Trabajo final de graduación].

Universidad de Costa Rica (UCR). (2010). *Informe 2010: Hacia la Sociedad de la Información y el Conocimiento*. PROSIC.

Universidad de Costa Rica (UCR). (2024). *Implementación de un sistema de detección de URLs maliciosas en tiempo real* [Trabajo final de maestría].

Universidad de Costa Rica (UCR), Escuela de Ciencias de la Computación e Informática (ECCI). (s. f.). Página institucional. https://www.ecci.ucr.ac.cr/

Universidad Empresarial de Costa Rica. (s. f.). Técnico en Ciberseguridad. https://uempresarial.com/tecnico-en-ciberseguridad/

Universidad Estatal a Distancia (UNED). (s. f.). Ingeniería Informática. https://www.uned.ac.cr/ecen/carrera/ii/88

Universidad Fidélitas. (s. f.). Bachillerato en Ingeniería en Seguridad Informática (Ciberseguridad) y Técnico Especializado en Ciberseguridad. https://ufidelitas.ac.cr/carrera/ingenieria-en-seguridad-informatica/

Universidad La Salle. (s. f.). Programa de Técnico en Ciberseguridad. https://www.ulasalle.ac.cr/tecnicos-22/#1638941978617-5f3a600c-1189

Universidad Latina de Costa Rica. (s. f.). Licenciatura en Seguridad Informática y Técnico en Ciberseguridad. https://www.ulatina.ac.cr/oferta-academica/ingenierias-y-tics/seguridad-informatica

Universidad Nacional de Costa Rica (UNA). (s. f.). Ingeniería en Sistemas de Información. https://www.carreras.una.ac.cr/ingenieria-en-sistemas-de-informacion/

Universidad San Marcos. (s. f.). Licenciatura en Sistemas Informáticos. https://www.usanmarcos.ac.cr/licenciatura/sistemas-informaticos

Universidad Técnica Nacional (UTN). (s. f.). Ingeniería en Software y Tecnologías Informáticas. https://www.utn.ac.cr/content/ingenieria-software-tecnologias-informaticas

Universae. (s. f.). Centro de investigación y ciberseguridad UNIVERSAE en Costa Rica (CI-CI). https://universae.com/descubre-nuestro-centro-de-investigacion-y-ciberseguridad-universae-en-costa-rica-ci-ci/#

Universae. (s. f.). Página principal. https://universaeuniversidad.cr/

ULACIT. (s. f.). ULACIT lanza nueva carrera de bachillerato en Ciberseguridad [Nota institucional]. https://www.ulacit.ac.cr/noticias/ulacit-lanza-nueva-carrera-de-bachillerato-en-ciberseguridad/

UNODC – United Nations Office on Drugs and Crime. (2012). *The Commission on Crime Prevention and Criminal Justice*. http://www.unodc.org/unodc/en/frontpage/2010/April/crime-congress-wraps-up-with-salvador-declaration.html

UNA UNIVERSIDAD NACIONAL COSTA RICA

LABORATORIO DE I+D+i LABCIBE EN CIBERSEGURIDAD

VICERRECTORÍA DE INVESTIGACIÓN UNIVERSIDAD NACIONAL

Anexo I

Glosario de términos clave en ciberseguridad

Activo de información

Elemento que tiene valor para una organización y que debe ser protegido. Incluye información, datos, sistemas, servicios, infraestructura tecnológica, personas y procesos que participan en el tratamiento de la información.
(ISO/IEC 27000:2022)

Amenaza informática

Causa potencial de un incidente no deseado que puede resultar en daño a un sistema, organización o persona, mediante la explotación de una vulnerabilidad.
(ISO/IEC 27000:2022; NIST SP 800-30)

Ataque cibernético

Intento deliberado de comprometer la confidencialidad, integridad o disponibilidad de un sistema de información, red o activo digital, mediante técnicas como malware, ingeniería social, explotación de vulnerabilidades o ataques de denegación de servicio.
(NIST SP 800-61; NIST CSF)

Ciberseguridad

Preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio. Comprende la protección de sistemas, redes y datos frente a amenazas que se originan en entornos digitales interconectados.
(ISO/IEC 27032:2012; NIST CSF)

Confidencialidad

Propiedad que asegura que la información no esté disponible ni sea divulgada a personas, entidades o procesos no autorizados.
(ISO/IEC 27000:2022)

Control de seguridad

Medida administrativa, técnica u organizativa implementada para modificar el riesgo de ciberseguridad. Los controles pueden ser preventivos, detectivos o correctivos.
(ISO/IEC 27000:2022; NIST SP 800-53)

Datos personales

Cualquier información relacionada con una persona física identificada o identificable, directa o indirectamente, conforme a la normativa nacional vigente en materia de protección de datos.
(Alineado con ISO/IEC 27701 y legislación nacional)

Disponibilidad

Propiedad que garantiza que los usuarios autorizados tengan acceso oportuno y confiable a la información y a los sistemas de información cuando sea requerido.
(ISO/IEC 27000:2022)

Gestión del riesgo de ciberseguridad

Proceso coordinado para dirigir y controlar una organización con respecto a los riesgos relacionados con la ciberseguridad, incluyendo la identificación, análisis, evaluación y tratamiento del riesgo.
(ISO/IEC 27005:2022; NIST SP 800-30)

Incidente de ciberseguridad

Evento o conjunto de eventos que comprometen, o tienen una probabilidad significativa de comprometer, la confidencialidad, integridad o disponibilidad de la información o de los sistemas de información.
(ISO/IEC 27000:2022; NIST SP 800-61)

Integridad

Propiedad que asegura la exactitud y completitud de la información y de los métodos de procesamiento.
(ISO/IEC 27000:2022)

Marco normativo de ciberseguridad

Conjunto de leyes, reglamentos, directrices, políticas y estándares que regulan y orientan la gestión de la ciberseguridad a nivel institucional o nacional.
(Alineado con NIST CSF – Govern Function)

Política de ciberseguridad

Declaración formal de la alta dirección que establece principios, objetivos, roles y responsabilidades para la gestión de la ciberseguridad dentro de una organización.
(ISO/IEC 27001:2022)

Riesgo de ciberseguridad

Combinación de la probabilidad de ocurrencia de un incidente de ciberseguridad y la magnitud de sus consecuencias sobre los activos de información.
(ISO/IEC 27005:2022; NIST SP 800-30)

Vulnerabilidad

Debilidad de un activo o control que puede ser explotada por una amenaza para causar daño a la organización.
(ISO/IEC 27000:2022; NIST SP 800-30)

Las definiciones contenidas en este glosario se basan principalmente en las normas ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27005 y en los marcos conceptuales del National Institute of Standards and Technology (NIST), con el fin de asegurar consistencia terminológica, rigor metodológico y comparabilidad internacional en el análisis del estado de la ciberseguridad.

ISBN: 978-9968-526-27-2

VICERRECTORÍA DE INVESTIGACIÓN
UNIVERSIDAD NACIONAL

LABORATORIO DE I + D + i
LABCIBE
EN CIBERSEGURIDAD

UNA
UNIVERSIDAD NACIONAL
COSTA RICA