ESTADO DE LA CIBERSEGURIDAD EN COSTA RICA 2024

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 2024* / Edgar Vega Briceño, Roberto Lemaitre Picado, Alex Villegas Carranza, Celia María Solís Cordoncillo.
Universidad Nacional, Sede Regional Chorotega, 2025.
1 recurso en línea (100 páginas) : archivo de texto, PDF.

ISBN 978-9968-526-25-8

1.SEGURIDAD (INFORMÁTICA). 2. ANALISIS DE LA INFORMACIÓN. 3. REDES SOCIALES EN LÍNEA. 4. INTERNET 5. PROTECCIÓN DE DATOS. 6. PROPIEDAD INTELECTUAL.
I. Lemaitre Picado, Alex, coautor. II. Solís Cordoncillo, Celia María, coautora.
III. Título.

Autores
Edgar Vega Briceño
Roberto Lemaitre Picado
Alex Villegas Carranza
Celia María Solís Cordoncillo

Sede Regional Chorotega
Mayo, 2025

Índice

Presentación

El segundo informe "Estado de la Ciberseguridad en Costa Rica 2024" presenta los hallazgos derivados de la encuesta sobre el Estado de la Ciberseguridad en el país, enfocándose en áreas cruciales como la situación jurídica, la investigación, el desarrollo e innovación (I+D+i). Esta investigación fue realizada 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).

Es claro que la ciberseguridad se ha consolidado como un pilar esencial en sociedades cada vez más interconectadas, reconociéndose al ciberespacio como un entorno crítico dentro de la gestión de los riesgos de seguridad nacional. En este contexto, resulta imprescindible obtener una fotografía lo más precisa de la situación de la ciberseguridad en Costa Rica a través de un informe de acceso público.

Este estudio profundiza en la investigación, el desarrollo e innovación (I+D+i) en ciberseguridad, así como en los marcos regulatorios que guían este ámbito en el país, abordando temas como el delito informático y el proceso penal relacionado, teniendo como principal objetivo realizar un diagnóstico anual sobre la ciberseguridad en Costa Rica y presentar sus resultados a diversos actores clave: autoridades del sector público y privado, organismos de seguridad nacional, empresas tecnológicas, académicos, investigadores y grupos organizados de la sociedad civil.

Al ofrecer un análisis detallado de la situación actual, el informe busca ser una herramienta útil para la formulación de políticas públicas, la planificación estratégica y la implementación de medidas efectivas para la prevención y respuesta ante incidentes cibernéticos.

Edgar Vega Briceño

Coordinador LabCIBE

Introducción

En la era digital actual, la hiperconectividad y la evolución acelerada de las tecnologías han transformado radicalmente el panorama de la seguridad informática. Los ciberataques se han vuelto más sofisticados y frecuentes, con amenazas que evolucionan constantemente desde el *ransomware* hasta los ataques de día cero, exponiendo vulnerabilidades críticas en infraestructuras esenciales. En este contexto, donde la superficie de ataque se expande exponencialmente, la ciberseguridad ha dejado de ser una opción para convertirse en un imperativo estratégico, fundamental para la supervivencia y competitividad empresarial en un ecosistema digital interconectado.

La digitalización masiva de procesos y servicios, junto con la adopción generalizada de tecnologías emergentes como la nube, Internet de las cosas (IoT por sus siglas en inglés) y la inteligencia artificial, ha creado un escenario donde los vectores de ataque se multiplican diariamente. Las organizaciones enfrentan amenazas persistentes avanzadas (APTs), campañas de ingeniería social cada vez más convincentes y ataques a la cadena de suministro que pueden comprometer múltiples objetivos simultáneamente. Esta realidad ha evidenciado que la ciberseguridad debe abordarse desde una perspectiva holística, integrando tecnología, procesos y, crucialmente, el factor humano como primera línea de defensa.

Este estudio busca realizar un análisis exhaustivo del estado de la ciberseguridad en Costa Rica, evaluando la madurez de las organizaciones en aspectos críticos como la gestión de riesgos cibernéticos, la respuesta a incidentes, la continuidad del negocio y el cumplimiento regulatorio. Mediante una metodología que combina análisis cuantitativos y cualitativos, se pretende establecer un diagnóstico preciso que permita identificar brechas de seguridad significativas y oportunidades de fortalecimiento en el ecosistema nacional de ciberseguridad.

El informe mantiene la estructura de iniciar con un análisis del marco jurídico y normativo que regula la ciberseguridad en Costa Rica, incluyendo estándares internacionales relevantes y mejores prácticas de la industria. Posteriormente, examina el estado actual de la investigación y desarrollo en ciberseguridad, considerando tanto iniciativas públicas como privadas. El diagnóstico situacional se fundamenta en datos empíricos recopilados mediante encuestas y evaluaciones técnicas, culminando con recomendaciones estratégicas para fortalecer la postura de ciberseguridad nacional, alineadas con estándares globales y adaptadas al contexto local.

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

La arquitectura de la ciberseguridad se fundamenta en tres pilares esenciales:

1. **Confidencialidad:** este pilar garantiza que la información sea accesible únicamente a entidades y procesos autorizados. Se implementa mediante:
   - Sistemas de cifrado de datos que convierten la información en formatos indescifrables para usuarios no autorizados
   - Mecanismos robustos de control de acceso que combinan autenticación y autorización
   - Redes Privadas Virtuales (VPN) que establecen canales seguros de comunicación
2. **Integridad:** asegura la exactitud y completitud de la información, protegiéndola contra modificaciones no autorizadas. Se mantiene a través de:
   - Implementación de firmas digitales y funciones *hash* criptográficas
   - Sistemas de control de versiones para el seguimiento de cambios
   - Protocolos de gestión de accesos y registros de auditoría
3. **Disponibilidad:** garantiza el acceso continuo y confiable a los recursos de información cuando sean requeridos. Se logra mediante:
   - Implementación de sistemas redundantes y copias de respaldo
   - Mecanismos de protección contra ataques de denegación de servicio
   - Programas de mantenimiento preventivo y actualizaciones sistemáticas

1.1.1 ¿Qué son las amenazas informáticas?

Se define como amenaza informática, cualquier acción o suceso capaz de perjudicar nuestros sistemas, redes o información. Estas varían en su forma y fines, abarcando desde el hurto de datos personales hasta el colapso de infraestructuras críticas, por tanto, algunos ejemplos de riesgos cibernéticos incluyen:

- **Virus y *malware*:** constituyen programas perjudiciales que buscan sustraer, dañar o eliminar datos, en el caso de los virus, se refiere a aquellos que se replican y diseminan autónomamente, mientras que *malware* es el término genérico para *software* nocivo como troyanos, gusanos y *ransomware*.
- ***Phishing*:** táctica de engaño para que las víctimas desvelen información confidencial como contraseñas o detalles financieros.
- **Ataques de fuerza bruta:** intentos reiterados de descifrar contraseñas o claves hasta lograr acceso.
- **Ataques DDoS:** consisten en sobrecargar un sistema o servicio específico con un flujo masivo de tráfico de datos, este tráfico proviene de diversas fuentes, a menudo computadoras o dispositivos comprometidos por *software* malicioso, como troyanos. El objetivo de estos ataques es saturar la capacidad de respuesta del sistema, lo que impide el acceso regular al servicio o sitio web afectado.
- **Exploits:** utilización de fallas en *software* o *hardware* para infiltrarse o provocar daños.
- **Intercepciones man-in-the-middle:** cuando un atacante se infiltra en una comunicación entre dos partes de manera encubierta.

Las amenazas siempre están vinculadas a vulnerabilidades, las cuales incrementan el riesgo de que dichas amenazas se materialicen. En esta cadena de sucesos, el ataque cibernético explota la vulnerabilidad para ejecutar la amenaza.

1.2 Marco Regulatorio de la Ciberseguridad en Costa Rica

El desarrollo del marco jurídico en materia de ciberseguridad en Costa Rica ha experimentado una evolución significativa, impulsada por el incremento exponencial en la conectividad digital y el aumento correlativo de incidentes cibernéticos. Las estadísticas del Organismo de Investigación Judicial (OIJ) evidencian esta tendencia preocupante, mostrando un incremento sostenido en las denuncias por delitos informáticos entre 2018 y 2024.

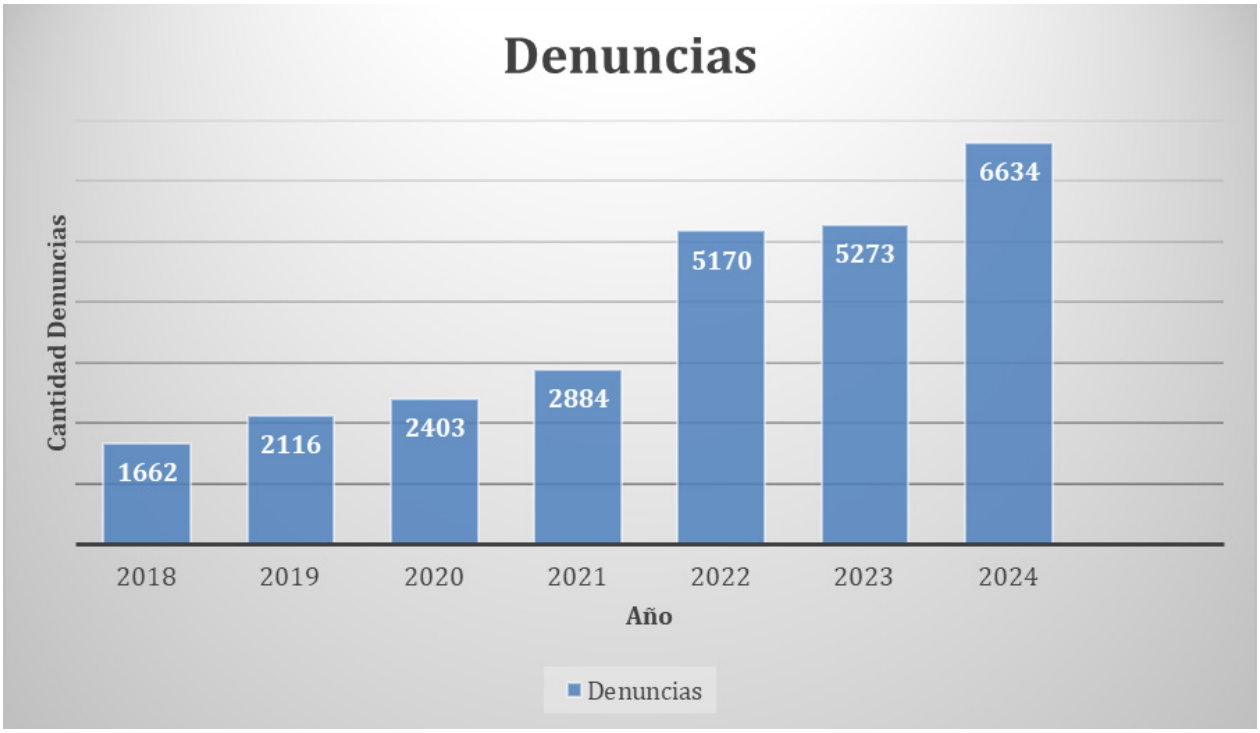
El análisis de los datos revela un aumento dramático en los incidentes reportados, pasando de 1,662 denuncias en 2018 a 6,634 en 2024 (hasta octubre), lo que representa un incremento superior al 300%. Este crecimiento exponencial ha catalizado el desarrollo de un marco regulatorio más robusto, que combina medidas punitivas con estrategias preventivas para abordar la ciberseguridad de manera integral.

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

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

Fuente: Unidad de Análisis Criminal OIJ 2024

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



Fuente: Unidad de Análisis Criminal OIJ 2024

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

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

Fuente: Unidad de Análisis Criminal OIJ 2024

No obstante, pese a que existen estos delitos informáticos y los temas de ciberseguridad siguen siendo tema recurrente entre el personal de tecnología, como se puede observar cada año aumenta la cantidad de delitos informáticos que ocurren en el país, ante este contexto se han generado medidas legales que buscan la persecución penal como acciones técnicas para buscar la prevención de incidentes informáticos, a continuación, se presenta la revisión del estado actual del país en materia jurídica:

1.2.1 Leyes

En esta sección se aborda contenido normativo cuya descripción no ha sufrido modificaciones significativas respecto al informe previo, Estado de la Ciberseguridad en Costa Rica 2023 (Vega et al., 2024). En consecuencia, partes del texto son reproducidas textualmente desde dicho informe, dada la continuidad de la normativa aplicable en este período. Estas citas literales se incluyen de manera intencional para mantener la precisión y coherencia de la información presentada. De igual forma se ha incluido nueva normativa que surgió dentro del periodo de revisión y que se analiza dentro de la sección.

1.2.1.1 Ley de la Administración Financiera de la República y Presupuestos Públicos N.º 8131[1]

Esta ley establece las normativas económico-financieras para la gestión de fondos públicos y se aplica a varias entidades:

1 Vega Briceño, E., Lemaitre Picado, R., Villegas Carranza, A., & Solís Cordoncillo, C. M. (2024). *Estado de la Ciberseguridad en Costa Rica 2023*. Universidad Nacional, Costa Rica.

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:** principios específicos del título II de la Ley y a 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 concreto se establecen dos artículos relacionados con el tema de ciberseguridad, sentando responsabilidades por acciones en contra del *hardware* como 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.

Como se puede observar, ambos artículos reflejan una preocupación significativa por la integridad, seguridad y correcto funcionamiento de los sistemas informáticos de la Administración Financiera y de Proveeduría.

1.2.1.2 Ley de Certificados, Firmas Digitales y Documentos Electrónicos N.° 8454 y su Reglamentos[2]

En su Artículo 1°, se establece el ámbito de aplicación de la normativa referente a transacciones y actos jurídicos que involucran el uso de certificados, firmas digitales y documentos electrónicos, determinando que la ley se aplica a una amplia gama de transacciones y actos jurídicos, tanto en el ámbito público como en el privado, de esta forma abarca una variedad de situaciones legales y comerciales, desde contratos hasta acuerdos, siempre que se realicen digitalmente y no presenten excepciones tales como:

- **Disposición legal contraria:** en caso de existir alguna otra ley específica que regule o prohíba el uso de documentos electrónicos o firmas digitales en ciertos casos, dicha ley prevalecerá sobre esta.
- **Incompatibilidad con la naturaleza o requisitos del acto:** si la naturaleza del acto jurídico o sus requisitos específicos no son compatibles con el uso de medios electrónicos o digitales, entonces esta ley no se aplicará. Por ejemplo, algunos actos jurídicos pueden requerir expresamente la presencia física de las partes o la entrega de documentos en papel.

Es válido resaltar que la ley autoriza expresamente al Estado y a todas las entidades públicas a utilizar certificados digitales, firmas digitales y documentos electrónicos dentro de sus respectivas áreas de competencia, lo que implica que todas las operaciones del gobierno y sus diversas ramas pueden incorporar estas tecnologías digitales para agilizar procesos, mejorar la seguridad y la eficiencia en la gestión de documentos y transacciones, no obstante, lo anterior constituye un reto, pues hasta la fecha en muchas instituciones la aplicación de la normativa se ha atrasado, y en algunos casos dificultado. Siendo que se asegura en la misma ley que estos documentos con

2 Vega Briceño, E., Lemaitre Picado, R., Villegas Carranza, A., & Solís Cordoncillo, C. M. (2024). *Estado de la Ciberseguridad en Costa Rica 2023*. Universidad Nacional, Costa Rica.

firma digital certificada sean legalmente equivalentes a los tradicionales en papel, un principio conocido como equivalencia funcional. Esto se especifica en:

> *Artículo 3.- Reconocimiento de la equivalencia funcional.*
> *Cualquier manifestación con carácter representativo o declarativo, expresada o transmitida por un medio electrónico o informático, se tendrá por jurídicamente equivalente a los documentos que se otorguen, residan o transmitan por medios físicos.*

La ley también otorga valor probatorio a los documentos digitales firmados, especialmente importante en contextos legales, siendo de especial interés para el sector financiero del país:

> *Artículo 4.- Calificación jurídica y fuerza probatoria.*
>
> *Los documentos electrónicos se calificarán como públicos o privados, y se les reconocerá fuerza probatoria en las mismas condiciones que a los documentos físicos.*
>
> *Artículo 10.- Presunción de autoría y responsabilidad.*
>
> *Todo documento, mensaje electrónico o archivo digital asociado a una firma digital certificada se presumirá, salvo prueba en contrario, de la autoría y responsabilidad del titular del correspondiente certificado digital, vigente en el momento de su emisión.*
>
> *Artículo 11.- Alcance.*
>
> *Entiéndase por certificado digital el mecanismo electrónico o digital mediante el que se pueda garantizar, confirmar o validar técnicamente:*
>
> *a) La vinculación jurídica entre un documento, una firma digital y una persona.*
> *b) La integridad, autenticidad y no alteración en general del documento, así como la firma digital asociada.*
> *c) La autenticación o certificación del documento y la firma digital asociada, únicamente en el supuesto del ejercicio de potestades públicas certificadoras.*

1.2.1.3 Ley de protección de la niñez y la adolescencia frente al contenido nocivo de internet y otros medios electrónicos N° 8934[3]

En cuanto a la Ley N° 8934, la normativa establece el marco regulatorio para locales con acceso público a computadoras e Internet, enfocándose en el uso que se realice

3 Vega Briceño, E., Lemaitre Picado, R., Villegas Carranza, A., & Solís Cordoncillo, C. M. (2024). *Estado de la Ciberseguridad en Costa Rica 2023*. Universidad Nacional, Costa Rica.

por menores de edad, en esencia, la normativa describe las siguiente definiciones claves:

- **Internet y Sitio:** la ley ofrece una definición integral de Internet y lo que constituye un sitio web, permitiendo de esta forma entender el alcance de la ley en términos de qué recursos en línea están regulados.
- **Filtro:** define las herramientas utilizadas para controlar el acceso a contenido en Internet, destacando su importancia para proteger a los menores de contenido inapropiado.
- **Programa, navegador y programa de intercambio:** estas definiciones abarcan el *software* utilizado para acceder e interactuar con Internet, incluyendo el intercambio de archivos.
- **Foro virtual:** reconoce los espacios en línea donde los menores pueden interactuar con otros, y que requieren de supervisión o regulación.
- **Salario base y establecimientos:** estas definiciones son importantes para aspectos administrativos y de cumplimiento, especialmente en lo que respecta a las sanciones o multas y los lugares en que aplica la ley.
- **Otras formas de comunicación en red:** amplía el alcance de la ley más allá de la navegación web para incluir diversas formas de comunicación digital, como el correo electrónico, el chat y las videoconferencias.
- **Pornografía:** aclara la definición de pornografía, siendo este aspecto una de las preocupaciones principales al regular el acceso a Internet de los menores en locales.
- **Destinado a personas menores de edad:** esta definición es clave para determinar qué locales están sujetos a la ley, enfatizando que cualquier lugar accesible a menores, independientemente de su propósito principal, está incluido.

Según esta normativa, en sus artículos 4, 5 y 6, los encargados de la supervisión corresponden a la Superintendencia de Telecomunicaciones, la cual tendrá la fiscalización, la regulación y el control de los requerimientos y las estipulaciones establecidos en la ley, además de resolver los procedimientos administrativos por incumplimientos y sus sanciones, certificar a los locales libres de pornografía y contenidos nocivos.

Además, en su artículo 7, se establece una obligación de los proveedores de servicios de Internet referente a los filtros de contenido, y se agrega otra obligación 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, 2011)*

Además, contempla la educación tecnológica, en su artículo 8 señala que:

> *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.*

Dado el rápido avance de la tecnología, esta ley debería revisarse integralmente para asegurar que sigue siendo relevante y efectiva en un entorno digital en constante cambio, siendo que se pensó en los contextos de "cafés internet", locales que antes eran muy comunes que ofrecían el servicio de computadores con conexión a internet para navegar por los usuarios a cambio de un pago.

1.2.1.4 Ley de protección de la persona frente al tratamiento de sus datos personales N.° 8968 y su Reglamento[4]

En el contexto actual, donde el robo o el mal uso de datos personales se ha vuelto una preocupante realidad, nuestro país ha implementado desde el 2011 la Ley de protección de la persona frente al tratamiento de sus datos personales N.° 8968. Esta legislación tiene como objetivo principal proporcionar protección legal a los ciudadanos frente a la gestión de sus datos personales, además, establece las acciones jurídico-técnicas para el manejo de bases de datos, tanto por entidades públicas como privadas:

> *Artículo 1 - Objetivo y Finalidad. Esta ley de carácter público tiene como finalidad asegurar a todas las personas, sin importar su nacionalidad, residencia o domicilio, la protección de sus derechos fundamentales. Esto incluye, de manera específica, el derecho a la autodeterminación informativa en lo que respecta a la vida privada o actividades personales, así como la salvaguarda de la libertad e igualdad en el tratamiento de sus datos personales, ya sea de manera automatizada o manual.*
>
> *Artículo 2 - Ámbito de Aplicación. La ley se aplica a los datos personales contenidos en bases de datos automáticas o manuales, tanto de entidades públicas como privadas. Sin embargo, no se aplica a bases de datos mantenidas por individuos o entidades con fines exclusivamente personales, internos o domésticos, siempre que estos no se vendan o comercialicen.*

4 Vega Briceño, E., Lemaitre Picado, R., Villegas Carranza, A., & Solís Cordoncillo, C. M. (2024). *Estado de la Ciberseguridad en Costa Rica 2023*. Universidad Nacional, Costa Rica.

La normativa desarrolla aspectos claves en materia de protección de datos, tales como:

- **Autodeterminación informativa:** este principio, resaltado en los artículos 4 y 5, otorga a las personas el derecho a controlar la información que proporcionan, cómo se utiliza y el tratamiento general de sus datos personales.
- **Calidad de la información:** la Ley impone a instituciones públicas y privadas el deber de asegurar que la información que manejan sea actual, veraz y precisa, garantizando la corrección y relevancia de los datos personales.
- **Medidas de seguridad y protección de datos:** determine que las entidades deben implementar protocolos y medidas técnicas y organizativas para asegurar la seguridad de los datos personales, lo cual implica proteger la información contra alteración, destrucción accidental o ilegal, pérdida, y acceso o tratamiento no autorizado. Estas medidas deben estar en línea con los avances tecnológicos actuales para garantizar una protección efectiva.
- **Registro y supervisión:** las bases de datos que no cumplan con estos estándares no podrán registrarse ante la Agencia de Protección de Datos de los Habitantes (PRODHAB), creada por esta ley, siendo la responsable de supervisar el cumplimiento de la normativa sobre datos personales de Costa Rica, buscando así una práctica efectiva de la ley.

Actualmente, en la Asamblea Legislativa se encuentran en análisis y discusión varios proyectos en materia de protección de datos para buscar actualizar la normativa nacional con el fin de adaptarla y adecuarla a las últimas actualizaciones a nivel mundial que han surgido, principalmente con el Reglamento Europeo de Protección de Datos, el cual ha generado una nueva visión más amplia en protección de datos y es el que ha marcado el "norte" a todos los países para actualizar y remozar esta materia.

1.2.1.5 Código Penal Ley N° 9048: Reforma de varios artículos y modificación de la sección VIII, denominada delitos informáticos y conexos, del título VII del Código Penal[5]

La reforma del Código Penal en Costa Rica, en el 2012 y 2013, marca un avance significativo en la búsqueda de luchar contra el cibercrimen, en el sentido que introduce nuevas categorías penales que abordan específicamente delitos cometidos en Internet, aquellos que anteriormente carecían de un marco para su denuncia y procesamiento; con estos cambios, Costa Rica se ha colocado a la vanguardia entre los países que han reformado de manera integral su legislación penal en el ámbito de los delitos informáticos. Sin embargo, es importante reconocer que aún persisten

5 Vega Briceño, E., Lemaitre Picado, R., Villegas Carranza, A., & Solís Cordoncillo, C. M. (2024). *Estado de la Ciberseguridad en Costa Rica 2023*. Universidad Nacional, Costa Rica

ciertas deficiencias, especialmente en la aplicación práctica de estos nuevos tipos penales en el contexto informático y de que nuestro Organismo de Investigación Judicial cuente con recursos suficientes para hacer frente a esta ciberdelincuencia en crecimiento.

Veamos algunos de los artículos:

Artículo 196.- Violación de correspondencia o comunicaciones.

Será reprimido con pena de prisión de uno a tres años a quien, con peligro o daño para la intimidad o privacidad de otro, y sin su autorización, se apodere, acceda, modifique, altere, suprima, intervenga, intercepte, abra, entregue, venda, remita o desvíe de su destino documentación o comunicaciones dirigidas a otra persona.

La misma sanción indicada en el párrafo anterior se impondrá a quien, con peligro o daño para la intimidad de otro, utilice o difunda el contenido de comunicaciones o documentos privados que carezcan de interés público.

La misma pena se impondrá a quien promueva, incite, instigue, prometa o pague un beneficio patrimonial a un tercero para que ejecute las conductas descritas en los dos párrafos anteriores.

La pena será de dos a cuatro años de prisión si las conductas descritas en el primer párrafo de este artículo son realizadas por:

a) Las personas encargadas de la recolección, entrega o salvaguarda de los documentos o comunicaciones.
b) Las personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

(Reformado por el artículo 1.° de la ley N.° 9135 del 24 de abril de 2013. Publicado en el Alcance N.° 78 a la Gaceta N.° 80 del 26 de abril de 2013)

Artículo 196 bis.- Violación de datos personales.

Será sancionado con pena de prisión de uno a tres años quien en beneficio propio o de un tercero, con peligro o daño para la intimidad o privacidad y sin la autorización del titular de los datos, se apodere, modifique, interfiera, acceda, copie, transmita, publique, difunda, recopile, inutilice, intercepte, retenga, venda, compre, desvíe para un fin distinto para el que fueron recolectados o dé un tratamiento no autorizado a las imágenes o datos de una persona física o jurídica almacenados en sistemas o redes informáticas o telemáticas, o en contenedores electrónicos, ópticos o magnéticos.

La pena será de dos a cuatro años de prisión cuando las conductas descritas en esta norma:

a) Sean realizadas por personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.
b) La información vulnerada corresponda a un menor de edad o incapaz.
c) Las conductas afecten datos que revelen la ideología, la religión, las creencias, la salud, el origen racial, la preferencia o la vida sexual de una persona.

No constituye delito la publicación, difusión o transmisión de información de interés público, documentos públicos, datos contenidos en registros públicos o bases de datos públicos de acceso irrestricto cuando se haya tenido acceso de conformidad con los procedimientos y limitaciones de ley.

Tampoco constituye delito la recopilación, copia y uso por parte de las entidades financieras supervisadas por la Sugef de la información y datos contenidos en bases de datos de origen legítimo de conformidad con los procedimientos y limitaciones de ley".

(Adicionado por Ley N.° 8148 de 24 de octubre de 2001 y posteriormente reformado en la forma indicada por el artículo 1.° de la ley N.° 9135 del 24 de abril de 2013. Publicada en el Alcance N.° 78 a la Gaceta N.° 80 del 26 de abril de 2013)

Artículo 217 bis. - Estafa informática

Se impondrá prisión de tres a seis años a quien, en perjuicio de una persona física o jurídica, manipule o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos, programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro.

La pena será de cinco a diez años de prisión, si las conductas son cometidas contra sistemas de información públicos, sistemas de información bancarios y de entidades financieras, o cuando el autor es un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

Indiscutiblemente, los delitos informáticos representan una amenaza creciente a nivel global, y ningún país, incluido el nuestro, está exento de este fenómeno de

criminalidad. En términos jurídicos, especialmente en el ámbito penal y otras ramas del derecho, aún queda mucho por desarrollar para abordar adecuadamente y de manera actualizada estos desafíos.

Expertos en seguridad informática advierten que muchos ataques cibernéticos pueden estar pasando desapercibidos, esta situación representa un riesgo significativo para las organizaciones, ya que la falta de detección y respuesta adecuada a los ataques cibernéticos puede llevar a consecuencias severas. Estas incluyen pérdidas financieras, violaciones regulatorias, incumplimiento en la gestión de la información, daño a la reputación de la marca y pérdida de confianza por parte de clientes y el público en general. Por lo tanto, se hace cada vez más necesario un enfoque integral y actualizado en la ciberseguridad, que no solo se centre en la prevención, sino también en la detección y respuesta efectiva a los incidentes de seguridad cibernética.

1.2.1.6 Adhesión de la República de Costa Rica al Convenio de Europa sobre Ciberdelincuencia[6]

El Convenio de Budapest, firmado el 21 de noviembre de 2001 y ratificado por 45 países, es un acuerdo internacional crucial en el ámbito de la ciberdelincuencia. Este convenio, adoptado por el Comité de Ministros del Consejo de Europa y en vigor desde el 1 de julio de 2004, es el único tratado internacional que abarca todas las áreas relevantes de la legislación sobre ciberdelincuencia, incluyendo derecho penal, procesal y cooperación internacional.

Costa Rica ratificó el Convenio mediante la Ley N° 9452 del 26 de mayo de 2017, promoviendo una política penal común contra la ciberdelincuencia y fomentando la cooperación internacional con el fin de buscar generar una efectiva persecución judicial.

Es importante destacar, que Costa Rica estableció tres cláusulas interpretativas, mediante el Alcance N° 202 del 18 de agosto del 2017, en el Diario Oficial la Gaceta, por medio del Decreto Ejecutivo N° 4546-RREE., relacionadas con delitos contra la propiedad intelectual, la extradición de costarricenses por delitos informáticos y la designación de un "punto de contacto" para asistencia en investigaciones de ciberdelincuencia, designando al Poder Judicial para esta función.

En general, la importancia del Convenio de Budapest, en el contexto de la ciberdelincuencia, se puede desglosar en varios aspectos clave:

- El convenio proporciona un marco legal coherente y armonizado para la persecución de delitos cibernéticos, al establecer un conjunto común de leyes,

6 Vega Briceño, E., Lemaitre Picado, R., Villegas Carranza, A., & Solís Cordoncillo, C. M. (2024). *Estado de la Ciberseguridad en Costa Rica 2023*. Universidad Nacional, Costa Rica.

facilita la cooperación internacional en la investigación y procesamiento de estos delitos, que a menudo trascienden las fronteras nacionales.
- Define y tipifica una gama 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 la tecnología que hace que todos los países firmantes tengan un "piso común" de delitos penales en sus legislaciones
- El convenio fomenta la colaboración entre los países miembros, facilitando la asistencia legal mutua y el intercambio de información, esto es esencial dado que la naturaleza de la ciberdelincuencia a menudo implica actores y recursos distribuidos globalmente.

1.2.2 Decretos

1.2.2.1 Reglamento para la Protección de los Programas de Cómputo en los Ministerios e Instituciones Adscritas al Gobierno Central - N° 37549-JP

Este reglamento, aprobado en 2012 y con reformas posteriores, constituye un marco reglamentario, el cual procura asegurar el uso legal y responsable de los programas de cómputo en las entidades gubernamentales de Costa Rica, pues se basa en una serie 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.

De manera que, este reglamento busca que las instituciones públicas procuren prevenir y combatir 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 como internacional, de manera que, insta el establecimiento de sistemas y controles que permitan garantizar la utilización única y exclusivamente de programas autorizados en todos los equipos y programas necesarios por la institución, asegurando que la documentación se encuentre custodiada, asimismo, implica el registro constante de inventarios que incluya licencias, instalaciones y demás autorizaciones de esta índole, todo esto a fin de cumplir con la protección de derechos de autor.

En línea con lo anterior, establece que cada Ministerio e Institución adscrita al Gobierno Central, se encuentra en la obligación de realizar una auditoría anual que permita la determinación del cumplimiento con las disposiciones del presente reglamento, las cuales se encuentra intrínsecamente ligadas a la normativa de protección de los derechos de autor.

Además, deberán presentar un informe ante el Registro Nacional de Derechos de Autor y Derechos Conexos indicando detalladamente el grado de cumplimiento así como la cantidad de equipo disponible, siendo así, el Registro Nacional de Derechos

de Autor y Derechos Conexo constituye el ente responsable de dar seguimiento y cumplimento a cabalidad de los establecido en el Reglamento por medio del análisis de dichos informes, y en caso de incongruencias o incumplimiento escalar el informe a las autoridades pertinentes, en este caso el Ministro de Justicia y Paz.

1.2.2.2 Creación Comisión Internet Costa Rica, CI-CR[7]

Adscrita al Ministerio de Ciencia, Tecnología y Telecomunicaciones, esta Comisión se encarga de recomendar políticas y directrices estratégicas relacionadas con Internet en Costa Rica. Además, reconoce que Internet trasciende las fronteras nacionales, lo que requiere un enfoque global en el desarrollo de políticas.
Su artículo 1 señala el fin de esta Comisión:

> *Artículo 1°-Créase la Comisión Internet Costa Rica, CI-CR, adscrita al Ministerio de Ciencia Tecnología y Telecomunicaciones (*) (MICITT)(*) con el fin de recomendar las políticas y directrices estratégicas relacionadas con el uso y desarrollo de Internet en Costa Rica.*
>
> *Para el funcionamiento de la CI-CR se utilizarán los recursos tanto financieros como humanos ya existentes en la Institución y en las demás instituciones que la conformen.*
>
> *(*)(Modificada su denominación por el artículo 11 de la Ley "Traslado del sector Telecomunicaciones del Ministerio de Ambiente, Energía y Telecomunicaciones al Ministerio de Ciencia y Tecnología", N° 9046 del 25 de junio de 2012)*

Esta Comisión es importante en el tema de ciberseguridad en el tanto cumpla lo que estipula su fin el artículo 3 inciso c, en el campo de recomendaciones técnicas y de seguridad en el uso de Internet en el país:

> *Artículo 3°—Los objetivos específicos de la CI-CR serán:*
>
> > *c) Promover estudios y recomendar procedimientos y normas técnicas y operacionales para asegurar el funcionamiento eficiente de las redes y servicios de Internet, así como su adecuada y creciente utilización por la sociedad costarricense.*

1.2.2.3 Creación de la Comisión Nacional de Seguridad En Línea N.° 36274-MICIT

En 2010, se estableció la Comisión Nacional de Seguridad en Línea en Costa Rica, la cual tiene como objetivo principal desarrollar políticas efectivas para el uso apropiado de Internet y las Tecnologías Digitales. Aunado a esto, se enfoca en abordar los riesgos

7 Vega Briceño, E., Lemaitre Picado, R., Villegas Carranza, A., & Solís Cordoncillo, C. M. (2024). *Estado de la Ciberseguridad en Costa Rica 2023*. Universidad Nacional, Costa Rica.

asociados con el uso de Internet, por lo que, uno de sus roles clave es participar en la creación y coordinación del Plan Nacional de Seguridad en Línea. La Comisión está integrada por varias entidades clave:

- Ministerio de Ciencia y Tecnología, que asume la presidencia;
- Ministerio de Educación Pública;
- Ministerio de Cultura y Juventud;
- Superintendencia de Telecomunicaciones;
- Poder Judicial;
- Patronato Nacional de la Infancia;
- Fundación Paniamor; la Fundación Omar Dengo (FOD);
- Cámara Costarricense de Tecnologías de la Información y la Comunicación (CAMTIC).

Es prudente señalar, que la Comisión sesionará al menos una vez al mes cuando sea convocada por su presidente, y además la Comisión podrá invitar en calidad de observadores a otras instituciones o actores que considere relevantes.

1.2.2.4 Creación del "Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR)" N.° 37052-MICIT[8]

El "Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR)" fue establecido en 2012 por el decreto N° 37052-MICIT del Ministerio de Ciencia y Tecnología de Costa Rica, y tiene como misión principal coordinar con diversas entidades del Estado, incluyendo instituciones autónomas, empresas y bancos estatales, en todo lo concerniente a la seguridad informática y cibernética. Además, su propósito es formar un grupo de expertos en seguridad de Tecnologías de la Información para prevenir y responder a incidentes de seguridad cibernética que afecten a las instituciones gubernamentales.

El artículo 2 del decreto establece varios objetivos esenciales para el CSIRT-CR, incluyendo la promoción de la cultura de seguridad cibernética a nivel nacional, la coordinación de acciones para mejorar la seguridad cibernética, el apoyo a autoridades en la investigación de delitos cibernéticos, y la colaboración con entidades nacionales e internacionales en el desarrollo de políticas y estrategias en este ámbito.

El CSIRT-CR, bajo la supervisión del Ministerio de Ciencia y Tecnología, tiene una amplia gama de responsabilidades y actividades, estas incluyen asesorar en la creación de políticas y estrategias de seguridad cibernética, promover la implementación

8 Vega Briceño, E., Lemaitre Picado, R., Villegas Carranza, A., & Solís Cordoncillo, C. M. (2024). *Estado de la Ciberseguridad en Costa Rica 2023*. Universidad Nacional, Costa Rica.

de estas políticas en las instituciones gubernamentales, elaborar planes de trabajo anuales, preparar informes de incidentes, y llevar a cabo acciones de capacitación en seguridad cibernética con expertos nacionales e internacionales.

El Consejo Directivo del CSIRT-CR está integrado por representantes de diversos ministerios y entidades, incluyendo al Ministro de Ciencia y Tecnología, quien preside el consejo, así como representantes de los ministerios de la Presidencia, Seguridad Pública, Relaciones Exteriores, Justicia y Paz, y la Academia Nacional de las Ciencias. El CSIRT-CR tiene un papel crucial en la protección de la infraestructura cibernética del país y en mejorar la ciberseguridad de todo el Estado.

1.2.2.5 Directriz N° 133-mp-micitt dirigida a la administración pública central y descentralizada sobre las mejoras en materia de ciberseguridad para el sector público del estado[9]

La Directriz N° 133-MP-MICITT, dirigida a la Administración Pública Central y Descentralizada, fue promulgada como respuesta a los ciberataques realizados por el grupo cibercriminal Conti en el año 2022 en Costa Rica. Su propósito es establecer acciones obligatorias instruidas por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) y el Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR) para fortalecer la ciberseguridad en la Administración Pública. De manera que, es evidente que esta directriz es crucial para que el Poder Ejecutivo ejerza su autoridad en la mejora de la ciberseguridad nacional, especialmente a través del MICITT, que actúa como ente rector en la gobernanza digital y la ciberseguridad. Las acciones fundamentales que establece la Directriz incluyen:

1. **Cumplimiento de recomendaciones técnicas:** seguir las instrucciones del MICITT y del CSIRT-CR relacionadas con la seguridad informática.
2. **Mejora de la resiliencia tecnológica:** esto implica actualizaciones constantes de sistemas, cambio de contraseñas en todos los sistemas institucionales, desactivación de servicios y puertos innecesarios, y un monitoreo efectivo de la infraestructura de red.
3. **Participación en formación y capacitación:** autorizar la asistencia del personal de ciberseguridad y equipos de TI a eventos organizados por el MICITT.
4. **Reporte de incidentes al CSIRT-CR:** informar al CSIRT-CR sobre cualquier incidente de seguridad que afecte la confidencialidad, disponibilidad, integridad de servicios públicos o la continuidad operativa.
5. **Documentación de incidentes:** respaldo de información relevante a incidentes para facilitar investigaciones futuras.

9 Vega Briceño, E., Lemaitre Picado, R., Villegas Carranza, A., & Solís Cordoncillo, C. M. (2024). *Estado de la Ciberseguridad en Costa Rica 2023*. Universidad Nacional, Costa Rica.

6. **Registro de sitios web:** informar al CSIRT-CR sobre todos los dominios de sitios web de las instituciones para su inclusión en el validador oficial de sitios del gobierno y prevenir suplantaciones y *phishing*.
7. **Análisis semestral de vulnerabilidades:** realización de dos análisis anuales de vulnerabilidades en los sitios web reportados y atender a las recomendaciones resultantes.
8. **Implementación de alertas técnicas:** aplicar las alertas técnicas emitidas por el CSIRT-CR en las instituciones y sus sistemas para reducir vulnerabilidades tecnológicas.

1.2.2.6 Decreto N° 46 H-MICITT "Instituciones del sector público privilegiarán la adquisición de soluciones de cómputo en la nube sobre otro tipo de infraestructura"[10]

Mediante el Decreto N° 46 H-MICITT, se establece que el sector público se encuentra en la obligación de privilegiar la adquisición de modelos de cómputo en la nube sobre otros tipos de infraestructura, en la medida que sea posible, conveniente y acorde a la naturaleza de las funciones, se aplica para equipos, licencia, bases de datos y sistemas informáticos, operativos, ofimáticos ya sea para el usuario final o para el centro de datos, lo anterior, a fin de facilitar el acceso a plataformas tecnológicas y digitales, además, pretende aumentar el alcance en materia de disponibilidad, en el sentido que, indiferentemente de la ubicación geográfica del usuario, este puede ingresar a dichas plataformas.

En atención a esta directriz, las instituciones públicas y demás órganos desconcentrados deberán incluir dentro de sus procesos de compra, la evaluación de servicios de esta índole como una opción adicional, en donde se detalle una valoración legal, financiera y técnica, esta última con mayor relevancia en torno a accesibilidad, funcionalidad, confidencialidad, transparencia, seguridad e inclusive integración y capacitación; de forma que, por medio de este proceso evaluativo se procura asegurar la calidad del servicio. Aunado a lo anterior, los jerarcas designados para cada entidad pública deberán realizar anualmente un informe técnico que puntualice el seguimiento de a dicha directriz y avances en torno a tecnologías de información y comunicaciones, a fin de mantener un registro actualizado y evitar inversiones innecesarias o redundantes, por tanto, para el proceso de registro de información, cada jerarca cuenta con la potestad de implementar el instrumental necesario, siempre y cuando no comprometa la seguridad de la información y la infraestructura tecnológica de la institución.

10 Vega Briceño, E., Lemaitre Picado, R., Villegas Carranza, A., & Solís Cordoncillo, C. M. (2024). *Estado de la Ciberseguridad en Costa Rica 2023*. Universidad Nacional, Costa Rica.

Este decreto busca que se logre generar eficiencia en el gasto público en materia tecnológica que puede generar el uso de plataformas y servicios en la nube, además de permitir que los equipos de tecnologías puedan dedicarse a otros temas en las instituciones y no solo centrarse en actividades de soporte y mantenimiento que puedan ser más rentables con servicios en la nube.

1.2.2.7 Directriz N.° 036-MTSS-MICITT, "Implementación de accesibilidad de la red de los sitios del sector público"

La Directriz sobre Accesibilidad de la Red de los Sitios del Sector Público, emitida conjuntamente por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) y el Ministerio de Trabajo y Seguridad Social (MTSS), establece un marco normativo fundamental para garantizar la inclusión digital en los servicios públicos digitales. Esta normativa responde a la necesidad de asegurar que toda la población, incluyendo personas con discapacidad, pueda acceder efectivamente a los recursos y servicios gubernamentales en línea.
El alcance de implementación de la directriz se estructura en dos niveles:

1. **Administración Pública Central:** establece la obligatoriedad de implementar estándares de accesibilidad web siguiendo los lineamientos técnicos establecidos por el Consejo Nacional de Personas con Discapacidad (CONAPDIS) y el MICITT.
2. **Administración Pública Descentralizada:** promueve la adopción de estos mismos estándares, fomentando un ecosistema digital público uniformemente accesible.

La directriz establece un marco de responsabilidades claramente definido:

- **MICITT y CONAPDIS:**
    - Desarrollo y actualización continua de lineamientos técnicos
    - Alineación con estándares internacionales de accesibilidad web
    - Supervisión de la implementación
- **Instituciones Públicas:**
    - Elaboración de planes de trabajo detallados
    - Establecimiento de cronogramas de implementación
    - Presentación de informes semestrales de avance y cumplimiento

Esta normativa se alinea con marcos legales nacionales e internacionales sobre derechos de las personas con discapacidad, fortaleciendo así el compromiso del Estado con la inclusión digital y la igualdad de oportunidades en la sociedad de la información.

1.2.2.8 Decreto N.° 44196-MSP-MICITT Reglamento sobre medidas de ciberseguridad aplicables a los servicios de telecomunicaciones basados en la tecnología de quinta generación móvil (5g) y superiores[11]

El decreto N.° 44196-MSP-MICITT 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. Este reglamento es aplicable a cualquier entidad, ya sean personas físicas o jurídicas, públicas o privadas, nacionales o extranjeras, que ofrezcan servicios de telecomunicaciones basados en tecnología 5G en el territorio nacional, excluyendo las redes privadas de telecomunicaciones.

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

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

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 seguridad nacional y a la protección del derecho a la intimidad, privacidad y el secreto de las comunicaciones

Si bien la idea es loable, este reglamento presenta varias preocupaciones y dudas. En principio se limita que equipos de empresas cuya sede está ubicada en países que

11 Vega Briceño, E., Lemaitre Picado, R., Villegas Carranza, A., & Solís Cordoncillo, C. M. (2024). *Estado de la Ciberseguridad en Costa Rica 2023*. Universidad Nacional, Costa Rica.

no se han adherido al Convenio de Europa sobre Ciberdelincuencia (Budapest, 2001) sean utilizados en "elementos críticos" de la red 5G "por representar un alto riesgo de ciberseguridad", lo cual va a ser considerado como parámetros de "alto riesgo" de ciberseguridad, esto contraviene el “principio de neutralidad tecnológica”, reconocido en la normativa legal y tratados internacionales suscritos por Costa Rica, donde este principio garantiza que los operadores de redes y proveedores de servicios de telecomunicaciones elijan libremente sus tecnologías, y se rijan por estándares de seguridad, que deben estar en un cartel, y como hemos visto anteriormente el Convenio de Budapest no es un estándar de ciberseguridad, este establece el marco de cooperación penal para persecución de delitos cibernéticos y que todos los firmantes establezcan en sus países una base común de delitos en sus códigos penales para poder cooperar.

1.2.3 Estrategia Nacional de Ciberseguridad MICITT 2023-2027[12]

La Estrategia Nacional de Ciberseguridad 2023-2027, presentada por el Gobierno de Costa Rica, aborda los desafíos y oportunidades que emergen en el contexto de los avances tecnológicos. Aunque estos avances han transformado significativamente la economía, la sociedad y la cultura, también han traído consigo retos en materia de seguridad, especialmente en lo que respecta a las tecnologías de información y comunicación, la creciente generación y almacenamiento de información, junto con la dependencia tecnológica, han incrementado los riesgos, amenazas y vulnerabilidades, exponiendo a los usuarios a diversos peligros.

Esta estrategia se desarrolla en respuesta a la necesidad de abordar de manera integral la seguridad cibernética, que se ha convertido en un aspecto crítico y transversal para la administración actual, en especial tras los ataques cibernéticos sufridos en 2022 que afectaron al sector público y llevaron a declarar un estado de emergencia nacional. Su objetivo es fortalecer la ciberseguridad a nivel nacional, impulsar la innovación y fomentar una cultura de seguridad robusta.

Los principales elementos de esta estrategia incluyen la articulación e implementación de mecanismos efectivos, la asignación adecuada de recursos y un sistema de rendición de cuentas. Además, esta estrategia busca no solo proteger la infraestructura crítica del país, sino también reafirmar el compromiso del estado en fortalecer sus capacidades para prevenir, mitigar y combatir las amenazas y delitos informáticos. En esencia, la Estrategia Nacional de Ciberseguridad 2023-2027 es un paso fundamental para garantizar la seguridad digital en Costa Rica en un entorno tecnológico en constante evolución.

12 Vega Briceño, E., Lemaitre Picado, R., Villegas Carranza, A., & Solís Cordoncillo, C. M. (2024). *Estado de la Ciberseguridad en Costa Rica 2023*. Universidad Nacional, Costa Rica.

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

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

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

Esta estrategia se estructura en torno a cinco pilares claves:

Pilar 1. Reforzar la gobernanza de ciberseguridad: busca que Costa Rica implemente un esquema de gobernanza para clarificar funciones, responsabilidades y métodos de interacción entre diversos actores. Esto incluye entidades gubernamentales, el sector privado, instituciones académicas, grupos organizados de la sociedad y colaboradores internacionales. El enfoque principal de este pilar es mejorar la coordinación general, fortalecer el liderazgo y optimizar los procesos de toma de decisiones relacionados con la ciberseguridad.

Pilar 2. Adecuar el marco jurídico cibernético: propone avanzar en el desarrollo de leyes y regulaciones específicas para el ámbito cibernético, complementadas con normativa técnica enfocadas en la ciberseguridad. Este pilar pretende establecer bases legales y regulatorias sólidas, destinadas a promover una gestión eficaz de los riesgos asociados a la ciberseguridad y a proporcionar las herramientas necesarias para contrarrestar las amenazas cibernéticas.

Pilar 3. Fortalecer la protección de infraestructuras y la ciberresiliencia nacional: pretende crear un sistema integral para el manejo de riesgos de ciberseguridad, el cual facilitará la identificación, reporte, análisis y respuesta rápida a incidentes relacionados con la ciberseguridad, además prioriza el desarrollo de habilidades 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 busca formar una fuerza laboral altamente capacitada en ciberseguridad mediante programas educativos, de entrenamiento y formación profesional, además de hacer

énfasis en elevar la conciencia sobre ciberseguridad entre la población, fomentando prácticas de comportamiento en línea responsables y seguras. Asimismo, impulsará la investigación y desarrollo en el campo de la ciberseguridad, con el objetivo de innovar, mejorar capacidades existentes y mantenerse al día frente a las amenazas cibernéticas que constantemente evolucionan. Este pilar subraya la importancia del desarrollo del capital humano y la participación del público, apuntando también a reducir la brecha de género en este sector laboral. Asimismo, propone promover 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: procura promover activamente la cooperación, tanto a nivel nacional como internacional, en temas de ciberseguridad, incluyendo así la colaboración y el intercambio de información relevante sobre este campo, buscando la participación en diversas iniciativas, alianzas y foros internacionales, con el objetivo de enfrentar amenazas cibernéticas que trascienden fronteras y contribuir al establecimiento de normativas globales en materia de seguridad cibernética.

De manera que, esta estrategia constituye una respuesta integral a los desafíos de la ciberseguridad en Costa Rica, buscando fortalecer la infraestructura, la cultura y la cooperación en el ámbito digital, el desarrollo de pilares y planes de acción son posibles de desarrollar, sin embargo, implica varios retos, entre ellos:

- **Recursos y financiamiento:** implementar una estrategia de ciberseguridad integral requiere una inversión significativa. Esto incluye no solo recursos financieros, sino también humanos y tecnológicos. El financiamiento debe ser sostenible a largo plazo para mantener y actualizar continuamente las capacidades de ciberseguridad, algo que en materia de ciberseguridad históricamente no se ha hecho.
- **Capacitación y desarrollo de talento:** la formación de una fuerza laboral calificada en ciberseguridad es esencial, esto implica no solo la capacitación inicial, sino también la educación continua para mantenerse al día con las amenazas en constante evolución, además de generar salarios atractivos para mantener el talento en ciberseguridad en el sector público.
- **Desarrollo y adaptación de legislación:** la creación de un marco legal adecuado es compleja y requiere equilibrar la protección y la privacidad, adaptarse a las realidades tecnológicas cambiantes y coordinarse con normas internacionales, y sobre todo mantener una versión integral, y no militarizada, que mantenga el equilibrio en materia de derechos humanos.

El reto es enorme y se necesitará un enfoque estratégico, colaboración entre diversos sectores, y un compromiso a largo plazo, aunque es un reto considerable, la implementación efectiva de estos pilares es fundamental para proteger la infraestructura nacional, las empresas y los ciudadanos contra las crecientes amenazas cibernéticas.

1.2.4 Estrategia de Transformación Digital 2023 - 2027

En un contexto global donde la digitalización se ha vuelto un elemento indispensable en la transformación de la industria e inclusive en los modelos de negocios, la Estrategia de Transformación Digital 2023-2027 pretende posicionar a Costa Rica como un referente en materia de innovación y desarrollo sostenible no solo a nivel nacional, sino también regional. Por tanto, su implementación dentro del marco de gobernanza digital permitiría aumentar la competitividad del país, estimular la cooperación entre actores claves y garantizar la inclusión digital para la población costarricense.

Aunado a ello, la estrategia se encuentra enfocada en la integración de tecnologías emergentes, el fortalecimiento de la infraestructura digital, la capacitación de la población costarricense, así como la promoción de alianzas público-privada. De manera que, al integrar las tecnologías emergentes en conjunto con un factor de sostenibilidad, se evidencia que la estrategia no solo busca eficiencia y desarrollo en términos económicos, sino también promover la transparencia gubernamental y la participación ciudadana, aspirando así a un futuro más interconectado, resiliente e inclusive próspero, en donde la tecnología catalice el crecimiento inclusivo y sostenible.

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

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

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

En cuanto al marco de gobernanza, la Estrategia de Transformación Digital 2023-2027 se fundamenta en un sólido marco de gobernanza que articula siete pilares esenciales, particularmente diseñados para orientar el proceso de transformación digital garantizando así su implementación efectiva y sostenible.

Pilar 1. Personas ciudadanas: enfocado en la creación de mecanismos inclusivos que permitan aumentar el acceso a las tecnologías emergentes.

Pilar 2. Interoperabilidad: interconectividad de los sistemas estatales.

Pilar 3. Ciberseguridad: asegurar la protección tanto de la información como de la infraestructura, generando seguridad y confianza.

Pilar 4. Marco de políticas: alinear estratégicamente las políticas públicas a fin de crear un marco integral, coherente y conciso.

Pilar 5. Marco jurídico: identificación del marco regulatorio que respalda el accionar público.

Pilar 6. Identidad digital y la firma digital certificada: herramientas clave para el acceso ciudadano a un Gobierno Digital.

Pilar 7. Digital por diseño: simplificación de procesos y generación de canales de comunicación y participación ciudadana.

1.2.5 Estrategia Nacional de Inteligencia Artificial 2024 - 2027

La Estrategia Nacional de Inteligencia Artificial 2024-2027 marca un hito en la transformación del país hacia un futuro innovador y sostenible, pues bajo la premisa de que IA se erige como el motor de la transformación digital e inclusive ha logrado redefinir las fronteras del progreso humano, Costa Rica se posiciona a la vanguardia con dicha estrategia, pues le permite abordar el desarrollo de la IA de manera estratégica, ética y efectiva, aprovechando así las oportunidades tanto para la industria como para la academia, y por ende aumentando el desarrollo económico. De este modo, le permite a Costa Rica no sólo posicionarse en el escenario internacional como un referente en el uso ético y responsable de esta tecnología emergente, sino también avanzar hacia un futuro en donde la IA no constituya únicamente una herramienta en el proceso de transformación, más bien genere oportunidades para el bien social y el desarrollo integral de la ciudadanía.

En virtud a ello, determina una serie de principios rectores fundamentales para guiar el desarrollo e implementación de la IA, minimizando así los riesgos implícitos mediante la creación de un marco ético que incentive la innovación, transparencia y equidad.

Principio 1. Paz y dignidad humana: operatividad de la IA con respeto a la dignidad humana, asegurando el desarrollo e implementación de la misma de manera ética y responsable, enfocado su funcionamiento a la generación del bienestar colectivo.
Principio 2. Supervisión humana: responsabilidad humana en la toma de decisiones mediante el cumplimiento de estándares éticos y jurídicos, así como el monitoreo y supervisión de algoritmos.

Principio 3. Transparencia y explicabilidad: bajo la premisa que el acceso a la información es un derecho constitucional, la implementación de la IA en instituciones gubernamentales debe ser transparente, auditable y apegada a principios de legalidad y rendición de cuentas. Asimismo, los actores que implementen o desarrollen esta tecnología deben proporcionar información accesible y comprensible que permita evidenciar tanto el impacto positivo como negativo.

Principio 4. Equidad y no discriminación: el diseño y operatividad de IA debe promover la inclusión y evitar la discriminación por religión, educación, género, etnia, edad, situación económica y orientación sexual, y por ende, reducir las brechas aún existentes en el país mediante la universalidad de la IA y el aumento inclusivo al acceso a tecnologías.

Principio 5. Responsabilidad: actores involucrados en el desarrollo, diseño e implementación de tecnologías de IA se encuentran en la responsabilidad de asumir las obligaciones éticas y jurídicas de sus operaciones, garantizando no solo una rendición de cuentas efectiva, sino también la supervisión humana en los procesos.
Principio 6. Sostenibilidad y bienestar: en virtud de los compromisos adquiridos en términos de sostenibilidad, los actores involucrados en el ciclo de vida de los sistemas de IA deben evaluar periódicamente los impactos resultantes del uso de estas tecnologías, asegurando la efectiva armonización tecnológica con el ambiente así como con la sociedad.

Principio 7. Seguridad, ciberseguridad y protección de la información: la operatividad de la IA debe desarrollarse de manera cibersegura y en protección a la ciudadanía y al país, por tanto, la identificación de riesgos y amenazas constituye un elemento fundamental en su funcionamiento. De esta manera, es evidente que implica el diseño y desarrollo de sistemas de IA robustos, seguros y confiables, por lo que es necesario la implementación de mecanismos de monitoreo, supervisión e inclusive intervención no solo para el máximo aprovechamiento de esta tecnología, sino también para fortalecer la privacidad de los datos.

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

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

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

1.2.6 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 establece los lineamientos fundamentales para robustecer las capacidades de protección digital del país. Esta iniciativa surge como respuesta estratégica ante el incremento de ciberataques contra la infraestructura tecnológica nacional, y se materializa a través de una significativa cooperación internacional con el Gobierno de los Estados Unidos de América, que ha destinado una donación de 25 millones de dólares para su implementación.

El núcleo del proyecto se centra en la creación y operación de un Centro de Operaciones de Seguridad (SOC), diseñado como una plataforma integral para la supervisión y gestión de la seguridad informática en las instituciones públicas. La implementación del proyecto sigue un enfoque en la selección de beneficiarios, priorizando instituciones responsables de infraestructuras críticas en sectores como energía, salud, transporte y comunicaciones. Esta selección estratégica reconoce la importancia fundamental de estos sectores para el funcionamiento socioeconómico del país y la seguridad nacional. El proceso de selección considera también la capacidad actual de las instituciones para gestionar riesgos cibernéticos, dedicando especial atención a aquellas que presentan mayores vulnerabilidades en sus sistemas de protección.

El Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR) asume un papel central en la ejecución del proyecto, coordinando tanto los aspectos técnicos como administrativos. Sus responsabilidades abarcan desde la distribución eficiente de recursos hasta la supervisión de la implementación tecnológica, incluyendo programas de capacitación y el desarrollo de documentación técnica especializada. La sostenibilidad a largo plazo constituye un pilar fundamental del proyecto. Las instituciones beneficiarias deben incorporar en su planificación presupuestaria los recursos necesarios para mantener y actualizar sus sistemas de ciberseguridad más allá del período inicial de apoyo. Esta previsión garantizaría la continuidad y efectividad de las medidas de protección implementadas, asegurando que la inversión inicial genere beneficios duraderos para la seguridad digital del país.

1.2.7 Marco Normativo de Gobierno y Gestión de las Tecnologías de Información (TI) en Costa Rica

El Marco Normativo de Gobierno y Gestión de las Tecnologías de Información constituye un pilar fundamental en la modernización digital del sector público costarricense. Este instrumento normativo, de carácter vinculante para todas las instituciones bajo la supervisión de la Contraloría General de la República, establece las directrices esenciales para garantizar una gestión tecnológica eficiente, segura y alineada con los objetivos estratégicos del Estado.

La estructura del marco se fundamenta en una delimitación de responsabilidades, donde los jerarcas institucionales asumen el liderazgo en la implementación y mantenimiento de las políticas establecidas, mientras que las Unidades de Tecnologías de Información ejecutan las operaciones técnicas y garantizan la resiliencia de los sistemas. Esta distribución de roles permite una gestión coherente y efectiva de los recursos tecnológicos, asegurando que las inversiones en tecnología generen valor público tangible.

El marco se estructura en cuatro ejes estratégicos interrelacionados que conforman un ecosistema integral de gestión tecnológica. El primer eje, la Gobernanza de TI, establece la necesidad de un órgano rector que coordine la estrategia tecnológica institucional, promueva la transparencia y asegure la alineación entre las iniciativas tecnológicas y los objetivos organizacionales. Este componente resulta crucial para garantizar que las decisiones tecnológicas respondan a las necesidades reales de las instituciones y sus usuarios.

La Gestión de TI, como segundo eje, define los procesos operativos necesarios para mantener servicios tecnológicos eficientes y confiables. Este elemento abarca desde la planificación estratégica hasta la implementación de arquitecturas empresariales robustas, estableciendo estándares de calidad que garanticen la efectividad de los

servicios digitales públicos. La gestión eficiente de estos recursos tecnológicos se convierte así en un catalizador para la modernización del Estado.

El tercer eje, centrado en Seguridad y Ciberseguridad, establece un marco robusto para la protección de activos digitales críticos. Esta dimensión resulta fundamental en un contexto de crecientes amenazas cibernéticas, estableciendo protocolos específicos para salvaguardar la confidencialidad, integridad y disponibilidad de la información gubernamental. La implementación de estas medidas de seguridad fortalece la confianza ciudadana en los servicios digitales del Estado.

La Continuidad Operativa, como cuarto eje, garantiza la resiliencia de los servicios públicos ante eventos disruptivos. Este componente asegura que las instituciones mantengan sus operaciones críticas incluso en situaciones adversas, mediante la implementación de planes de contingencia y recuperación ante desastres. Esta previsión resulta esencial para mantener la continuidad de los servicios públicos esenciales.

Para facilitar la implementación efectiva de estos ejes estratégicos, el marco proporciona un conjunto integral de herramientas y mecanismos de control. Estos instrumentos incluyen guías metodológicas, matrices de evaluación y perfiles de gestión que permiten a las instituciones evaluar y mejorar continuamente sus prácticas de gestión tecnológica. La aplicación sistemática de estas herramientas asegura una implementación coherente y efectiva del marco normativo en todas las instituciones públicas.

1.2.8 Código Nacional de Tecnologías Digitales (N°44507-MICITT)

El Código Nacional de Tecnologías Digitales (CNTD) representa una iniciativa estratégica del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) para establecer un marco normativo integral que regule la transformación digital del sector público costarricense. Este instrumento normativo define los estándares y buenas prácticas fundamentales para la adquisición, desarrollo y gestión de tecnologías digitales en las instituciones gubernamentales, con el propósito de garantizar servicios públicos más eficientes, accesibles y centrados en el ciudadano. La aplicación del CNTD tiene carácter vinculante para todas las entidades del sector público que desarrollen iniciativas o proyectos con componentes tecnológicos, exceptuando únicamente aquellos procedimientos relacionados con la defensa nacional y la seguridad del Estado. Esta obligatoriedad asegura una implementación uniforme de estándares tecnológicos en toda la administración pública, promoviendo la interoperabilidad y la coherencia en la prestación de servicios digitales.

El Código se fundamenta en el principio de democratización tecnológica, buscando garantizar que la transformación digital del Estado beneficie equitativamente a toda

la población. Este enfoque inclusivo se materializa a través de lineamientos específicos que aseguran la accesibilidad universal de los servicios digitales, considerando las diversas necesidades y capacidades de los usuarios. La normativa establece criterios claros para que las iniciativas tecnológicas no solo mejoren la eficiencia operativa, sino que también fortalezcan la transparencia y la participación ciudadana en la gestión pública.

Como órgano rector, el MICITT asume un papel fundamental en la implementación y supervisión del Código. Sus responsabilidades abarcan desde la promoción y difusión de las disposiciones normativas hasta el acompañamiento técnico a las instituciones en su proceso de adopción. El Ministerio desarrolla programas de capacitación continua para funcionarios públicos, asegurando que el personal responsable de implementar tecnologías digitales cuente con las competencias necesarias para garantizar su uso efectivo y seguro.

El alcance del CNTD se extiende a todas las fases del ciclo de vida de los proyectos tecnológicos, desde su conceptualización hasta su implementación y mantenimiento. Los lineamientos establecidos cubren aspectos críticos como la planificación estratégica, la gestión de riesgos, la seguridad de la información y la evaluación del impacto de las iniciativas digitales. Esta aproximación integral asegura que las inversiones en tecnología generen valor público tangible y contribuyan efectivamente a la modernización del Estado.

1.2.9 Regulación y Normalización de Adquisiciones de Tecnología y/o Desarrollo de Sistemas Informáticos de Apoyo a la Gestión (N° 053-H-MICITT)

La "Regulación y Normalización de Adquisiciones de Tecnología y/o Desarrollo de Sistemas Informáticos de Apoyo a la Gestión", emitida por el Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) en colaboración con el Ministerio de Hacienda, tiene como objetivo fundamental orientar a las entidades públicas en la adquisición eficiente de equipos tecnológicos y en el desarrollo de sistemas informáticos destinados a optimizar la gestión pública. Esta normativa busca asegurar el uso racional y transparente de los recursos del Estado, promoviendo la eficiencia en el gasto público y el cumplimiento estricto de las disposiciones legales y normativas que rigen la contratación de tecnología y servicios asociados.

El marco normativo establece que todas las entidades públicas, tanto de la administración central como descentralizada, deben cumplir con las Normas Técnicas de la Contraloría General de la República y con los lineamientos específicos emitidos por el MICITT para la adquisición de equipos electrónicos y la implementación de sistemas informáticos. En particular, se insta a priorizar el uso del "leasing operativo" (arrendamiento) como modalidad para la adquisición de equipos de cómputo,

siempre y cuando se haya realizado un análisis técnico que justifique su viabilidad y ventajas sobre otras alternativas disponibles.

Asimismo, se establece que los procedimientos de contratación administrativa deberán realizarse de manera obligatoria a través del Sistema Integrado de Compras Públicas (SICOP), lo que permite una gestión más ágil y transparente en la adquisición de bienes y servicios tecnológicos. En este contexto, se fomenta el uso de los convenios marco disponibles, los cuales ofrecen opciones estandarizadas para la adquisición de equipos y servicios, facilitando un proceso más eficiente y controlado. En cuanto a la 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 debe satisfacer las necesidades de las instituciones del sector público. Este convenio incluirá equipos como microcomputadoras de escritorio, portátiles y unidades de poder ininterrumpido (UPS), cuyas especificaciones técnicas serán aprobadas por el MICITT, garantizando que los equipos adquiridos cumplan con los estándares técnicos requeridos para el correcto funcionamiento de las entidades públicas.

Por último, 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 activa de otros órganos y entes del sector público en la observancia y ejecución de las disposiciones contempladas en la normativa.

1.2.10 Ley Marco de Acceso a la Información Pública (N° 10554)

La Ley Marco de Acceso a la Información Pública tiene como principal objetivo garantizar el ejercicio efectivo del derecho humano de acceso a la información pública en Costa Rica. Mediante esta ley, el Estado se compromete a promover la transparencia administrativa, reforzando la rendición de cuentas de las autoridades públicas y asegurando la publicidad de la función pública. Este marco normativo también extiende su alcance a los sujetos de derecho privado que posean información de interés público, quienes deben someterse a las disposiciones de la ley en la medida en que la información que gestionan incida en el ámbito público.

La ley se sustenta en una serie de principios fundamentales que guían la transparencia y el acceso a la información. El principio de transparencia establece que toda la información en poder de los sujetos obligados se presume pública, salvo que existan excepciones claramente establecidas por la ley. El principio de facilitación garantiza que los procedimientos para solicitar información sean accesibles y no constituyan un obstáculo para su obtención. Asimismo, el principio de rendición de cuentas impone a los funcionarios públicos la obligación de responder por su gestión y de hacer pública la información relevante sobre sus decisiones y acciones.

Además de estos principios, la ley incorpora otros valores clave, como la igualdad y no discriminación, asegurando que todas las personas tengan derecho a acceder a la información sin distinción alguna, y la gratuidad del acceso, evitando que los ciudadanos deban incurrir en costos adicionales para obtener información pública. El principio de máxima publicidad es especialmente relevante, pues establece que la información debe ser proactivamente proporcionada, actualizada y accesible para la ciudadanía.

La ley también define los límites al derecho de acceso, reconociendo que ciertos documentos pueden estar sujetos a restricciones bajo la legislación vigente. Sin embargo, estos límites deben ser interpretados de manera estricta, de forma que cualquier restricción al acceso debe estar debidamente justificada. En cuanto a la protección jurisdiccional, la ley establece que el acceso a la información pública puede ser impugnado mediante el recurso de amparo, en casos donde no se entregue la información dentro del plazo legal establecido o cuando la información proporcionada sea parcial, ambigua o incompleta.

Además, se establece la obligación de los sujetos obligados de publicar y mantener actualizada, de manera oficiosa, una serie de información pública de interés general. Entre la información que debe ser publicada se incluyen aspectos como la estructura orgánica de las instituciones, los servicios que brindan, los trámites administrativos, los salarios de los funcionarios públicos y otros informes relevantes. Además, la ley dispone que esta información debe ser accesible, incluyendo la provisión de formatos adecuados para personas con discapacidad.

En cuanto al acceso electrónico a la información pública, la ley regula este aspecto, asegurando que los sujetos obligados dispongan de un correo electrónico oficial y de un formulario accesible en sus sitios web, facilitando así la atención de solicitudes de información. También, se establece que los funcionarios deben incluir en sus informes anuales de labores los datos sobre las solicitudes de información pública recibidas, así como el seguimiento de la publicación proactiva de la información.

Por último, dispone que el Poder Ejecutivo deberá reglamentar esta ley dentro de un plazo de seis meses a partir de su promulgación. El transitorio único de la ley establece que todas las instituciones públicas deben actualizar la información en sus sitios web conforme a lo estipulado por la ley, en un plazo máximo de seis meses.

1.2.11 Acuerdo conassif 5-24 reglamento general de gobierno y gestión de la tecnología de información

El Acuerdo CONASSIF 5-24 establece un marco normativo crucial para la gestión de la Tecnología de la Información (TI) en las entidades financieras de Costa Rica, con el objetivo de garantizar la seguridad de la información y la adecuada gestión de los riesgos tecnológicos. En un contexto donde las tecnologías avanzadas, como la

computación en la nube y los sistemas interconectados, están desempeñando un papel cada vez más relevante, este acuerdo responde a los nuevos desafíos para la seguridad y la protección de datos sensibles, buscando minimizar las amenazas cibernéticas y garantizar la continuidad operativa de las entidades en un entorno cada vez más digitalizado.

Aspectos Clave del Acuerdo CONASSIF 5-24

1. **Gobernanza de TI:** el acuerdo subraya la importancia de contar con una estructura organizacional adecuada para la gobernanza de la Tecnología de la Información, destacando que los órganos de dirección deben ser responsables de la supervisión y la toma de decisiones estratégicas relacionadas con los riesgos tecnológicos. La alta gerencia de las entidades financieras tiene la responsabilidad de implementar políticas efectivas y medidas de control, con especial énfasis en los riesgos asociados a la ciberseguridad.
2. **Responsabilidad 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 tecnología de la información. Se les exige un compromiso claro con la protección de la privacidad y el secreto de las comunicaciones. Además, la alta gerencia debe poner en práctica medidas preventivas para gestionar los riesgos tecnológicos, asegurando una gestión eficaz y proactiva de los mismos.
3. **Ciberseguridad y protección de la información:** la seguridad de la información es uno de los ejes centrales del acuerdo. Se requiere que las entidades implementen mecanismos robustos para gestionar la ciberseguridad, incluyendo actividades como las pruebas de vulnerabilidad, el monitoreo constante y la respuesta ante incidentes. Se hace especial énfasis en proteger los tres pilares fundamentales de la seguridad de la información: la confidencialidad, la integridad y la disponibilidad de los datos.
4. **Uso de servicios en la nube y subcontratación de servicios:** el acuerdo regula el uso de servicios en la nube y la subcontratación de servicios tecnológicos, estableciendo que los proveedores deben cumplir con los estándares de ciberseguridad exigidos. Las entidades financieras deben garantizar que la gestión de la cadena de suministro sea segura, protegiendo así la infraestructura tecnológica crítica de posibles vulnerabilidades externas que pudieran comprometer la seguridad de la información.
5. **Auditoría y evaluación continua:** el acuerdo establece que las entidades deben realizar auditorías periódicas tanto internas como externas sobre sus sistemas de TI. Los auditores deben evaluar la efectividad de las políticas y controles implementados, y los resultados de estas auditorías deben ser reportados a las autoridades pertinentes para su análisis y seguimiento. Este proceso de auditoría es esencial para garantizar que las entidades se mantengan alineadas con las mejores prácticas en gestión de riesgos tecnológicos y ciberseguridad.

6. **Resiliencia operativa y continuidad del servicio:** se enfatiza la importancia de los planes de resiliencia operativa y la continuidad del servicio. Estos planes deben incluir estrategias para responder ante incidentes y recuperar la operatividad en casos de desastres tecnológicos. Se requiere que las entidades aseguren la continuidad de los servicios críticos, incluso en escenarios de crisis o emergencias.

1.2.12 Acuerdo SUGEF 10-07: Reglamento sobre Divulgación de Información y Publicidad de Productos y Servicios Financieros

El Acuerdo SUGEF 10-07 establece directrices claras para la divulgación de información y la publicidad de productos y servicios financieros en Costa Rica. Su principal propósito es garantizar la transparencia en las comunicaciones financieras y proteger a los consumidores, regulando de manera efectiva a las entidades supervisadas por la Superintendencia General de Entidades Financieras (SUGEF). Esta normativa tiene un enfoque integral, buscando mejorar la claridad de la información proporcionada a los usuarios y fortaleciendo la confianza de los consumidores en los productos financieros disponibles en el mercado.

Uno de los aspectos más relevantes del acuerdo es su énfasis en asegurar que la publicidad de los productos financieros sea veraz, clara y comprensible. Para ello, se exige que las entidades financieras proporcionen detalles completos sobre los costos asociados a los productos, tales como las tasas de interés, comisiones y otros gastos adicionales. De este modo, se garantiza que los usuarios puedan tomar decisiones informadas al contar con una imagen precisa de lo que realmente están adquiriendo. Además, se establece que la información publicada no debe inducir a error, por lo que se prohíben expresiones ambiguas que puedan generar malentendidos. Las tasas de interés y cuotas deben presentarse de manera uniforme y accesible para que todos los usuarios, sin importar su nivel de conocimiento financiero, puedan comprenderlas sin dificultad.

Otro componente de este reglamento es la divulgación transparente de información, que exige que las entidades mantengan actualizada y accesible la información sobre sus productos y servicios a través de sus plataformas digitales, principalmente sus sitios web. Esta información debe incluir tanto los precios mínimos como los máximos de los productos financieros, aclarando que estos son valores orientativos y pueden variar dependiendo del perfil del cliente. Es fundamental que las entidades financieras respeten estos lineamientos para evitar distorsionar la toma de decisiones de los usuarios, lo que contribuye a un entorno financiero más honesto y equitativo.
En cuanto a la prevención de estafas informáticas, el acuerdo marca un paso importante al exigir que, a partir de 2025, las entidades supervisadas implementen controles específicos para mitigar este tipo de riesgos. El acuerdo señala la importancia de adoptar medidas de ciberseguridad robustas, tales como la

implementación de la autenticación de múltiples factores, la protección de la información sensible del usuario y la notificación inmediata de cualquier actividad sospechosa. Además, las entidades deberán ofrecer programas de educación en ciberhigiene digital, asegurándose de que tanto los empleados como los usuarios estén conscientes de los riesgos informáticos y sepan cómo prevenirlos.

Las sanciones por incumplimiento también son una parte integral de este acuerdo. La normativa establece que las entidades que no cumplan con las disposiciones sobre divulgación de información y atención de quejas estarán sujetas a sanciones conforme a la Ley 7558 Ley Orgánica del Banco Central de Costa Rica. A través de este reglamento, se busca mejorar la relación entre las entidades financieras y sus usuarios, promoviendo una mayor equidad en el mercado.

Investigación y desarrollo de la ciberseguridad

CAPÍTULO II

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 aspecto de investigación y desarrollo, es importante reconocer a las organizaciones claves que invierten en (I+D) en el ámbito nacional, y tienen en su norte, la generación de nuevo conocimiento y la implementación de soluciones en seguridad cibernética. Entre estas se han reconocido 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 profesionales del sector de tecnologías de información y comunicación, 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 la ciberseguridad. Está orientada a desarrollar, divulgar y fortalecer el mercado de la ciberseguridad y tecnologías emergentes en Costa Rica y Latinoamérica. Su propuesta valor (CyberSec Clúster, s.f.), resalta los enfoques estratégicos del Clúster:

- 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 ha realizado una consulta para identificar las empresas especializadas en ciberseguridad que están 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 es un recurso valioso para comprender mejor el panorama actual y las capacidades en el sector de la 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 diseñados para proteger a sus clientes de una variedad de amenazas digitales. Los servicios que brindan incluyen, pero no se limitan a:

Consultoría en ciberseguridad: las empresas que caen en esta categoría ofrecen servicios de asesoramiento para ayudar a las organizaciones a entender y a manejar sus riesgos de ciberseguridad. Esto puede incluir el desarrollo de estrategias de ciberseguridad, la creación de políticas y la identificación de áreas de mejora.

Servicios administrados de seguridad (MSSP): algunas de estas empresas proporcionan servicios continuos de monitoreo y gestión de la seguridad de la red. Esto puede incluir la detección de intrusiones, la respuesta a incidentes y la gestión de sistemas de seguridad como *firewalls* y sistemas de detección de intrusiones.

Pruebas de penetración y análisis de vulnerabilidades: algunas compañías ofrecen este tipo de servicio, que implica probar activamente los sistemas de una empresa para identificar y solucionar vulnerabilidades de seguridad antes de que puedan ser explotadas por actores maliciosos.

Cumplimiento normativo y certificaciones: consultorio para brindar ayuda a las empresas a cumplir con las normas y certificaciones necesarias en su industria. Esto puede ser crucial para las empresas que operan en sectores altamente regulados o que manejan información sensible.

Formación y concienciación en ciberseguridad: algunas empresas ofrecen servicios de formación para ayudar a los empleados de sus clientes a entender y manejar los riesgos de ciberseguridad. Esta formación puede ser crucial para prevenir incidentes de seguridad causados por error humano.

Servicios de seguridad de red y *firewall*: algunas ofrecen soluciones de seguridad de red, incluyendo la implementación y gestión de *firewalls* de próxima generación (NGFW). Estos servicios son cruciales para prevenir accesos no autorizados a las redes de las empresas.

2.3 Ciberseguridad en la Academia

A fin de obtener una comprensión integral del panorama educativo y de investigación en el campo de la ciberseguridad en el país, es crucial identificar las universidades, tanto públicas como privadas, que se encuentran a la vanguardia en este sector. A continuación, se presenta una lista de universidades públicas y privadas que contribuyen al avance de la ciberseguridad en el país, por medio de sus programas académicos, proyectos de investigación y demás colaboración con la industria. Este panorama nos ofrece una visión clara de los esfuerzos educativos y de desarrollo en este campo.

2.3.1 Sector Público

CONARE: el Consejo Nacional de Rectores, representa una organización esencial en el ámbito educativo de Costa Rica, ya que está conformada por las cinco principales universidades públicas del país, con la particularidad de que dichas universidades son ampliamente reconocidas tanto por su excelencia académica como por su contribución significativa en el desarrollo de la investigación y la educación en Costa Rica. Siendo así, el papel de CONARE es fundamental en la coordinación y colaboración entre estas instituciones, promoviendo iniciativas que fortalecen la educación superior y la investigación, incluyendo áreas críticas como la ciberseguridad. Su labor no solo beneficia a las comunidades académicas y estudiantiles, sino que también impulsa el desarrollo social y tecnológico a nivel nacional. (CONARE, s.f.).

Las universidades son:

1. Universidad de Costa Rica (UCR)
2. Instituto Tecnológico de Costa Rica (TEC)
3. Universidad Nacional (UNA)
4. Universidad Estatal a Distancia (UNED)
5. Universidad Técnica Nacional (UTN)

Dentro de las universidades que forman parte de CONARE en Costa Rica, se ofrece una variedad de carreras directamente relacionadas con el área de la ciberseguridad, inclusive dichos programas académicos están diseñados para proporcionar a los estudiantes una educación integral y especializada, equipándolos con las habilidades y conocimientos necesarios para enfrentar los retos y demandas del campo de la ciberseguridad.

2.3.1.1 Instituto Tecnológico de Costa Rica (TEC)

En el año 2022, el TEC comenzó a ofrecer una Maestría en Ciberseguridad abierta con tres diferentes énfasis, los cuáles se enfocan en seguridad del *software*, defensa y ataque de sistemas, y gestión de la seguridad de la información. Además de su programa de maestría, el TEC también ofrece un programa Técnico en Ciberseguridad Empresarial, programa el cual está diseñado para proporcionar a los estudiantes una base sólida en la protección de los sistemas y la información corporativa. (TEC, 2022).

2.3.1.2 Universidad de Costa Rica (UCR)

La UCR no tiene un programa específico de ciberseguridad, pero su programa en Ciencias de Computación e Informática Empresarial puede incluir cursos relevantes. (UCR, s.f.).

2.3.1.3 Universidad Nacional (UNA)

Para 2025, se prevé la apertura de la Maestría en Ciberseguridad Industrial en la Sede Regional Chorotega, impulsada por el equipo de investigación, desarrollo e innovación (LabCIBE) (CRHoy, 2 de septiembre, 2024).

2.3.1.4 Universidad Técnica Nacional (UTN)

La UTN a la fecha no cuenta con un programa específico de ciberseguridad, aunque su programa de Ingeniería en Tecnologías de la Información incluye algunos cursos relevantes. (UTN, s.f.)

2.3.1.5 Universidad Estatal a Distancia (UNED)

La UNED no cuenta con un programa específico de ciberseguridad, aunque su programa de Ingeniería Informática incluye algunos cursos relevantes. (UNED, s.f.).

2.3.2 Sector Privado

CONESUP: el Consejo Nacional de Enseñanza Superior Universitaria Privada, juega un papel crucial en el sistema educativo de Costa Rica al regular y supervisar las universidades privadas del país, por lo que actualmente, hay 54 universidades privadas registradas bajo esta entidad. Entre estas instituciones, varias se destacan por ofrecer carreras, programas técnicos y especializaciones en el campo de la ciberseguridad. De manera que, esta oferta académica refleja un reconocimiento de la importancia creciente de la ciberseguridad en el panorama tecnológico y empresarial moderno. (CONESUP, s.f.)

2.3.2.1 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.)

2.3.2.2 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.)

2.3.2.3 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 seguridad cibernética (Universae, s.f.).*

2.3.2.4 Universidad Fidélitas

La Universidad Fidélitas ofrece un Bachillerato en Ingeniería en Seguridad Informática (Ciberseguridad) y un Técnico Especializado en Ciberseguridad. (Universidad Fidélitas, s.f.)

2.3.2.5 Lead University

Esta universidad ofrece un programa de Técnico Especializado en Ciberseguridad. (Lead University, s.f.)

2.3.2.6 Universidad La Salle

La Salle ofrece un programa de Técnico en Ciberseguridad. (Universidad La Salle, s.f.).

2.3.2.7 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.)

2.3.2.8 Ministerio de Educación Pública de Costa Rica

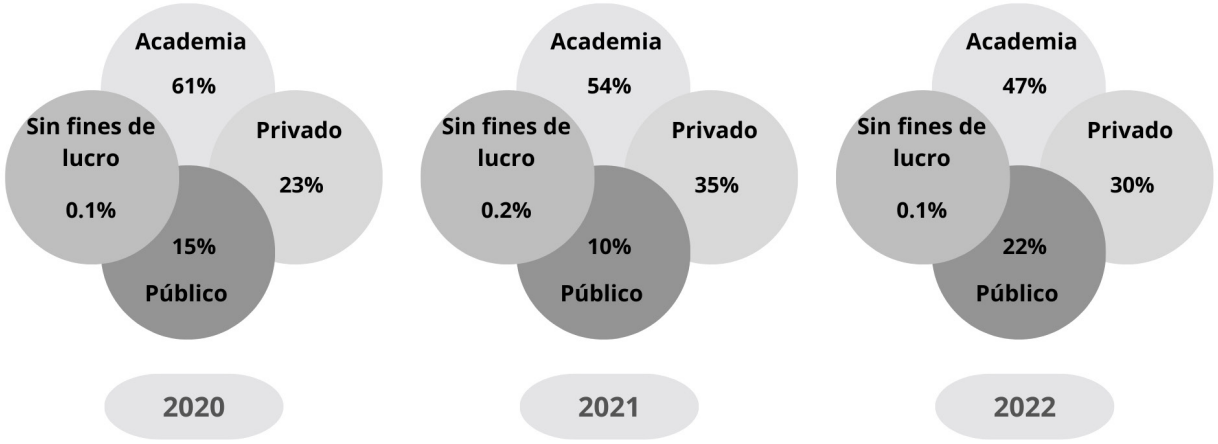
El MEP con el aval de CONESUP, ha estado ofreciendo un programa de Técnico en Ciberseguridad desde el año 2020. (Ministerio de Educación Pública de Costa Rica, 2020)

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.

2.4 Investigación y Desarrollo

En Costa Rica se destaca un estudio que da visibilidad a la inversión en I+D+i en diferentes campos de las Tecnologías de Información y la Comunicación (TIC); en el año 2022 el 0,34 por ciento del producto interno bruto (PIB) se destinó a esfuerzos de I+D y de este total, la academia ha invertido la mayor cantidad con un 47%, casi la mitad de toda la inversión en esta área. Es decir, la inversión en investigación y desarrollo está principalmente liderada por el sector académico. No hay datos específicos de cuál porcentaje de esta inversión se destina a Ciberseguridad.
En la siguiente imagen se pueden observar los montos de manera porcentual, con respecto a la totalidad de la inversión que se ha mantenido en un 0,34% del PIB durante los años 2020 hasta 2022.

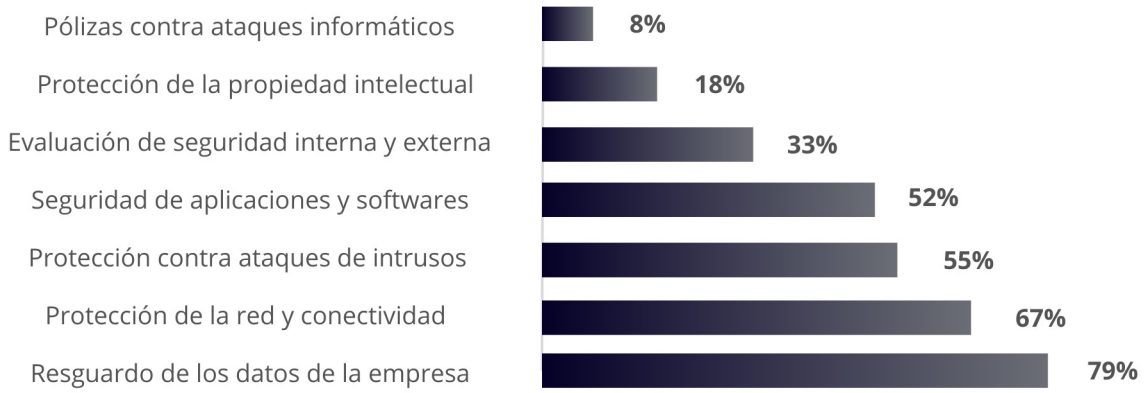
Figura 1. Distribución de Investigación y Desarrollo según sector



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

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

Figura 2. Procesos de seguridad informática



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

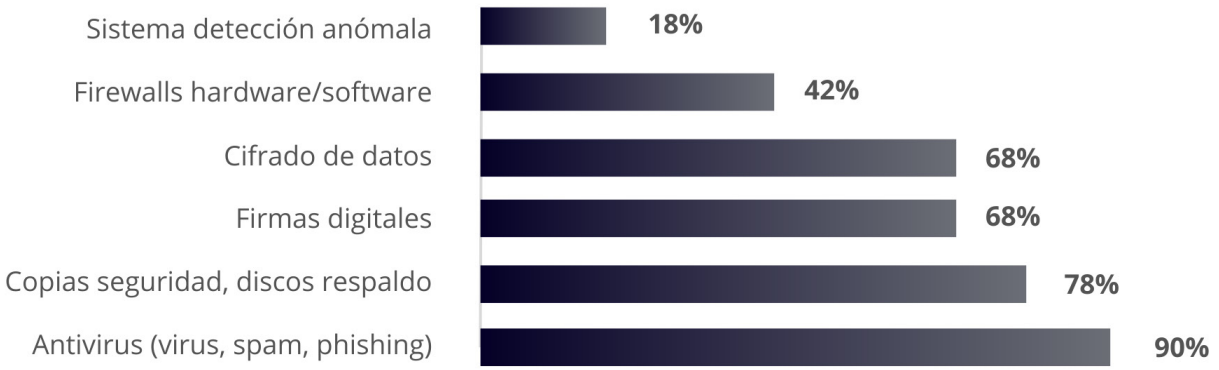
Esta imagen destaca los procesos de seguridad utilizados por organizaciones en Costa Rica. En menor medida están las pólizas contra ataques informáticos, protección de la propiedad intelectual, evaluaciones de seguridad internas y externas, mientras que en mayor medida pero aún con gran margen de mejora están la seguridad de aplicaciones y *software*, protección contra ataques de intrusos, la protección de la

red y conectividad llega a un 67% de las organizaciones, por encima de todos se encuentra el resguardo de los datos de la empresa siendo este el proceso que más se está implementando en las organizaciones del país con un 79%.

El resguardo de datos, protección de la red y protección contra ataques informáticos son los principales procesos de seguridad implementados en más del 55% de las organizaciones.

Una observación emitida en dicho estudio señala que las capas de mayor seguridad mostradas aquí son las menos utilizadas en las empresas.

Figura 3. Mecanismos de seguridad informática



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

Esta imagen muestra los mecanismos de seguridad informática utilizados en las organizaciones de Costa Rica, entre estos están los sistemas de detección de anomalías, siendo los menos utilizados con tan solo un 18% de uso entre las organizaciones muestreadas, los *firewalls* en *hardware* y *software* son utilizados en un 42% de las organizaciones, el cifrado de datos, firmas digitales, copias de seguridad, discos respaldo están más arriba en cuanto al uso. Mientras que el mecanismo de seguridad más utilizado son los antivirus con protección anti spam y *phishing*.

En resumen, antivirus, copias de seguridad, firmas digitales y cifrado de datos, son los principales mecanismos de seguridad utilizados en más del 68% de las organizaciones.

Algunos retos destacados en esta investigación son, la socialización de los procesos de seguridad informática, hay procesos críticos que tienen muy poca inversión y esto podría atribuirse a la falta de socialización o divulgación de estos temas. Aunado a esto, se debería promover más la inversión de I+D+i en el sector público y empresarial,

de acuerdo con el estudio, algunas de las dificultades que pueden explicar esta falta de inversión son la complejidad de tramitar acceso a financiamiento para I+D+i y la complejidad sobre patentar productos/servicios o procesos, pues según se menciona, obtener una patente puede representar un desafío significativo para los empresarios.

Aparte de este informe general, donde se mencionan aspectos importantes en la seguridad de la información, no existe un informe consolidado sobre el estado de la investigación y desarrollo en ciberseguridad en Costa Rica.

Otra fuente sobre la investigación en Ciberseguridad en Costa Rica es a través de los repositorios de las universidades públicas y privadas, estos repositorios son fuentes ricas de nuevas investigaciones y análisis, realizados por estudiantes y académicos especializados en ciberseguridad. Estos trabajos reflejan la investigación en curso y las contribuciones que se están realizando en el campo, ofreciendo una visión de los avances y desafíos en la ciberseguridad en un contexto costarricense y, por extensión, latinoamericano, por tanto, estas colecciones académicas son recursos invaluables para investigadores, profesionales y políticos interesados en entender y mejorar la ciberseguridad en la región.

Enlaces de repositorios con contenido de investigación en ciberseguridad:

- (Repositorio TEC, s.f.): https://repositoriotec.tec.ac.cr
- (Repositorio UNA, s.f.): https://www.siduna.una.ac.cr/index.php
- (Repositorio Cenfotec, s.f.): https://ucenfotec.librarika.com/search
- (Repositorio Universidad Latina, s.f.): https://repositorio.ulatina.ac.cr

Ante este contexto, es evidente que existe una necesidad en la creación de una oferta académica enfocada en dar respuesta a las nuevas necesidades y amenazas, por lo que se plantea ¿Qué tan complejo es crear estas carreras? A lo que, 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 otorgarán al completar la carrera.
5. **Análisis comparativo:** debe presentarse una comparación de la propuesta curricular con respecto a otras universidades 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.

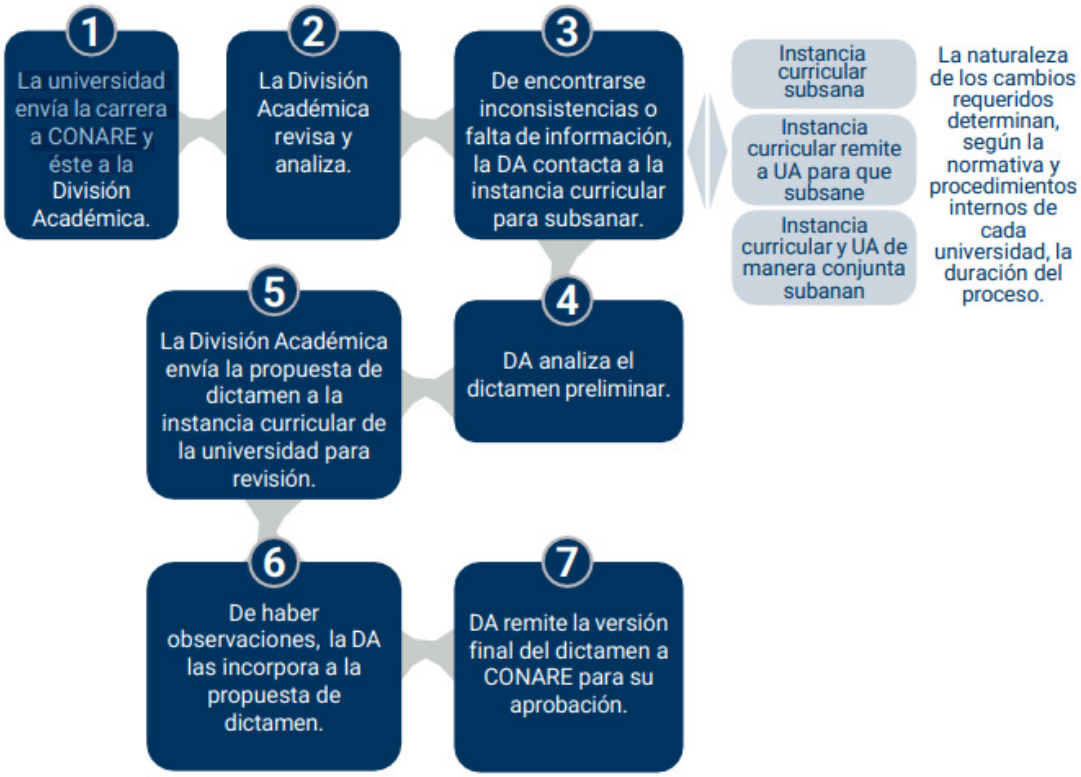
El proceso de apertura de una carrera virtual tiene requisitos compartidos con el proceso presencial, y además incluye:

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 de 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 4. 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 sobre la investigación del estado del arte de la Ciberseguridad Nacional en los aspectos de Investigación, Desarrollo y el estado Jurídico de la ciberseguridad en Costa Rica.

El **objetivo principal** del estudio es determinar anualmente el Estado de la Ciberseguridad en Costa Rica desde la perspectiva técnica, normativa y de gestión de manera general en el país por medio de consultas claves que nos permitan determinar de manera estadísticas el estado de situación para identificar los actuales desafíos y proponer recomendaciones que fortalezcan el entorno de ciberseguridad en el 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 pretende el diagnóstico sobre el estado de la ciberseguridad en Costa Rica desde una perspectiva jurídica, de investigación y desarrollo en ciberseguridad, e inclusive sobre aspectos de seguridad cibernética, prevención de incidentes informáticos, capacitación y formación en ciberseguridad así como recursos y presupuesto asignados. De manera que, se diseñó una encuesta en línea dirigida a varios actores vinculados con la I+D+i en el ámbito de la Ciberseguridad, implicando así el sector educativo costarricense, e incluso organizaciones de distintos ámbitos en la industria; lo anterior, a fin de obtener una perspectiva más amplia y detallada sobre la dimensión regulatoria, jurídica y el de la investigación y desarrollo de la ciberseguridad a nivel nacional.

Esta encuesta intenta identificar la existencia de programas o iniciativas que estimulen la investigación y desarrollo en la ciberseguridad, así como la postura de diferentes organizaciones con respecto al estado jurídico en relación a la ciberseguridad.

Encuesta 2024

Preguntas específicas sobre sobre el estado de I+D:

1.¿Ofrece su institución programas de formación o cursos específicos en Ciberseguridad? *

- O Si
- O No

Si su respuesta es "Sí", por favor especifique los programas o cursos ofrecidos:

---

2. ¿Mantiene su institución convenios con otras instituciones o empresas para la formación en ciberseguridad? *

- O Si
- O No

Si su respuesta es "Sí", por favor indique con quién mantiene estos convenios:

---

3. ¿Qué tan efectiva considera la implementación de dichos convenios y los resultados obtenidos?

- O Muy efectiva
- O Efectiva
- O Neutral
- O Poco efectiva
- O Nada efectiva

4. ¿Cuenta su institución con un presupuesto dedicado a actividades de investigación y desarrollo en Ciberseguridad?

- O Sí
- O No
- O Desconozco

5. En el último año, ¿Se han llevado a cabo investigaciones relacionadas a algún área de la ciberseguridad en su institución? *

- ○ Investigación
- ○ Desarrollo
- ○ Desconozco

6. ¿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):_____

7. ¿Cuenta su organización con planes futuros en términos de investigación y desarrollo en Ciberseguridad?

- ○ Si
- ○ No
- ○ Desconoce

8. ¿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
- ○ Otro

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

- ○ Muy Importante
- ○ Importante
- ○ Neutral
- ○ Poco Importante
- ○ No es Importante

10. ¿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
- ○ Neutral
- ○ En desacuerdo
- ○ Muy en desacuerdo

11. ¿Hay algo que le gustaría mencionar en relación al estado actual de la investigación y desarrollo de la ciberseguridad en su institución?

_____

_____

_____

_____

Preguntas específicas sobre la situación jurídica de la Ciberseguridad Nacional

Seguridad Cibernética

1. De las siguientes, ¿cuáles son sus mayores preocupaciones en seguridad cibernética?

- ○ Fraudes/Estafas informáticas
- ○ Pérdida de datos/Fuga de información
- ○ *Software* sin licencias/Piratas
- ○ Vulnerabilidades de *software* y sistemas
- ○ Concientizar a los usuarios
- ○ *Ransomware*
- ○ Ataques a la cadena de suministros

2. ¿Dispone la empresa de un seguro de ciberseguridad para protegerse frente a posibles incidentes informáticos?

- ○ Sí
- ○ No

3+ ¿Se encuentran interesado en adquirir un seguro de ciberseguridad?

- ○ Sí
- ○ No

3. ¿Ha sufrido alguno de los siguientes ataques en 2024?

- ○ 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

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

Estado de la Ciberseguridad

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

---

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

---

7. ¿En qué medida se involucra la alta dirección en las decisiones y políticas de ciberseguridad?

---

8. ¿Cómo se comunica la política de ciberseguridad y las mejores prácticas a los empleados?

---

9. De los siguientes mecanismos ¿cuales utiliza la institución para mantenerse actualizado sobre las recientes tendencias y amenazas que giran en torno a la ciberseguridad?

- ○ Participación en conferencias y/o seminarios
- ○ Participación en foros de ciberseguridad
- ○ Suscripción a bases de datos especializadas (revistas y publicaciones)
- ○ Consultoría externa
- ○ Programas de formación/capacitación
- ○ Otro

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

---

11. De los siguientes controles de seguridad cibernética ¿De cuáles dispone la empresa?

- ○ Firewall
- ○ Antispam
- ○ Antimalware
- ○ *Software* antivirus
- ○ *Backup* de información
- ○ Usuarios de autenticación en red
- ○ Herramientas de Detección de Incidentes (IDS, IPS, Auditorias y logs, EDR)
- ○ Active Directory on-Premise
- ○ Gestión de la Identidad en la Nube
- ○ Single Sign-on
- ○ Autenticación Multi Factor

12. ¿En qué puesto o departamento recae la responsabilidad de prevenir los incidentes informáticos en su institución?

---

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

---

14. ¿Se restringe en su empresa el acceso a la red desde dispositivos personales no gestionados?

---

15. ¿Existe algún reglamento, protocolo, política, directriz o circular donde se regule el uso de las Redes Sociales como Facebook, Twitter, Instagram, o alguna similar?

---

16. ¿La institución cuenta con medidas en materia técnica para cumplir la ley de protección de datos del cliente?

---

17. ¿Dónde considera que la mayor amenaza de ciberseguridad para su empresa/institución se origina?

---

18. En cuanto a dispositivos de almacenamiento externo (USB, discos duros), ¿cómo se gestionan en su institución?

- ○ Prohibidos
- ○ Permitidos pero restringidos
- ○ Permitidos sin restricciones
- ○ No se gestiona formalmente
- ○ No aplica
- ○ Desconoce

19. ¿Se realizan pruebas de *phishing* o simulacros de seguridad para evaluar la preparación de los empleados?

---

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

Programas de capacitación y/o formación

21. ¿La organización cuenta con iniciativas en materia de investigación y desarrollo en ciberseguridad I+D+i (investigación, desarrollo e innovación)

---

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

---

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

- ○ Ciberseguridad
- ○ Delitos informáticos
- ○ Protección de datos
- ○ Buenas prácticas de las tecnologías de información (TI)
- ○ Amenazas en línea
- ○ Gestión de incidentes de seguridad
- ○ Seguridad de contraseñas y autenticación de doble factor
- ○ Seguridad en dispositivos móviles y tecnologías inalámbricas
- ○ Redes sociales y protección de identidad digital
- ○ Ninguna

24. ¿Dispone la empresa de presupuesto para financiar certificaciones profesionales en ciberseguridad?

- ○ Sí
- ○ No
- ○ Desconoce

25. ¿La capacitación en ciberseguridad es de carácter obligatorio para todos los niveles de la organización?

- ○ Sí
- ○ No
- ○ Desconoce

26. ¿Ofrece la institución programas de formación continua en línea en ciberseguridad?

- ○ Sí
- ○ No

Procedimiento Legal

27. ¿Está familiarizado con la ley de delitos informáticos (Código Penal de Costa Rica)?

---

28. ¿Cree que esta ley cubre adecuadamente los incidentes informáticos en Costa Rica?

---

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

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

Recursos y Presupuesto

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

---

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

---

32. De la siguiente lista ¿La empresa subcontrata algún servicio relacionado con ciberseguridad? *

- ○ Monitoreo
- ○ Respuesta a incidentes
- ○ Evaluación de vulnerabilidades
- ○ Gestión de identidad y acceso
- ○ Auditorías de seguridad
- ○ Educación o concientización

Alcance Operativo

33. ¿Su empresa desarrolla actividades en mercados internacionales?

---

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

---

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

---

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

- ○ Sí
- ○ No
- ○ Desconoce

37. ¿La empresa utiliza alguna red privada virtual (VPN) o tecnologías de seguridad similares para proteger las comunicaciones de manera interna y externamente?

---

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

Inteligencia Artificial

39. ¿Utiliza su institución inteligencia artificial en procesos relacionados a la ciberseguridad?

- ○ Sí
- ○ No (condiciona siguientes)

40. 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
- ○ Investigación de incidentes
- ○ Protección de datos
- ○ Otro

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

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

42. ¿Cuáles considera los mayores desafíos en la implementación de herramientas de inteligencia artificial en ciberseguridad en su institución?

- ○ Integración de sistemas
- ○ Personal capacitado
- ○ Recursos presupuestarios
- ○ Privacidad y seguridad de datos
- ○ Escasez de datos
- ○ Otro

43. Dispone la empresa de personal calificado en inteligencia artificial

- ○ Sí
- ○ No

44. ¿Invierte su institución en formación y capacitación en inteligencia artificial aplicada a la ciberseguridad?

- ○ Sí
- ○ No

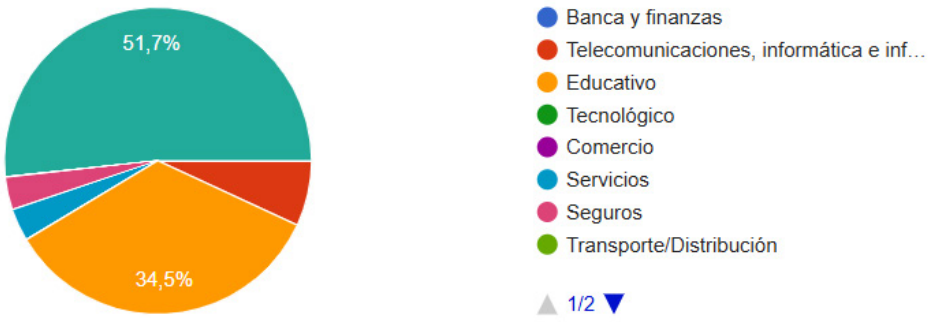
3.2 Resultados

A continuación, se presentan los resultados obtenidos en la edición 2024 de la encuesta, en la cual se recopilaron 29 respuestas de la variedad de actores invitados, proporcionando información relevante sobre el sector en donde desarrollan actividades. Cabe destacar que en el período actual, se evidencia una disminución en la participación en comparación con las 50 respuestas registradas previamente, estadísticamente esta reducción equivale a una variación del 42% menos en el número de participantes, y por tanto incidiendo en la distribución sectorial en contraste con la encuesta realizada en 2023.

En cuanto a los principales actores, los datos porcentuales revelan una distribución interesante entre los diversos sectores representados, en principio liderando el sector estatal con un 51,7%, evidenciando así un constante grado de participación e interés gubernamental en la evaluación estadística del estado de situación de la ciberseguridad en Costa Rica, y por ende reforzando su compromiso con la ciudadanía; en segundo plano se registra una participación del 34,5% por parte del sector educativo, participación muy similar a la edición 2023, esto como resultado del interés y compromiso de la academia en materia de I+D+i en tecnología.

Seguidamente, se puede observar una contribución menor pero significativa de otros sectores de relevancia, particularmente el sector de telecomunicaciones, informática e información representa un 6,9%, asimismo, tanto el sector de servicios como el de seguro representa respectivamente con un 3,4% cada uno.

Gráfico 1. Distribución de resultados por sector



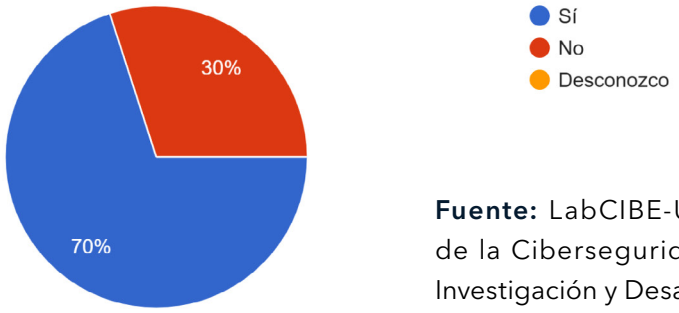
Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

3.2.1 Estado de la Investigación y Desarrollo en Ciberseguridad

La presente sección se dirige específicamente a la investigación y desarrollo de la ciberseguridad en instituciones académicas costarricenses, pues pretende recopilar información sobre la implementación de iniciativas y/o programas que estimulen la investigación y desarrollo en el área de la ciberseguridad, de manera que, únicamente comprende el 34,5% del total de encuestas realizadas. A continuación se proporciona una visión detallada sobre iniciativas, proyectos y programas en materia de ciberseguridad en instituciones educativas.

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

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



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

Sin embargo, los participantes detallaron los siguientes programas o cursos ofrecidos actualmente en sus instituciones educativas.

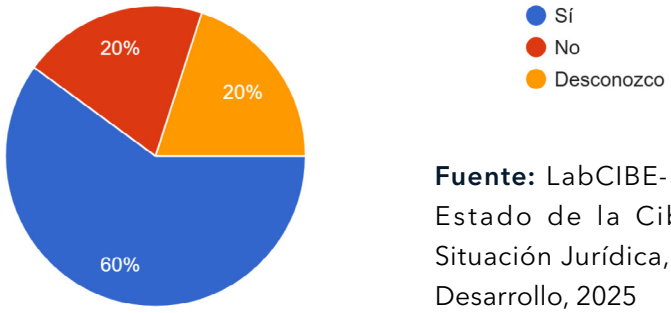
- Academia de Tecnologías, El CEA, CI y Metics acaban de completar el curso de Conciencia en Ciberseguridad que será de aplicación General en la Comunidad Universitaria.
- Técnico en Ciberseguridad, Licenciatura en Seguridad de la Información, curso de Fundamentos de Ciberseguridad, Curso de Introducción a la Ciberseguridad, Técnico Junior en Ciberseguridad de CISCO
- Técnico 3 en Ciberseguridad
- Bachillerato en Seguridad Informática, Especialización en Ciberseguridad
- Licenciatura en Sistemas Informáticos con énfasis en seguridad de la información
- Técnico y Maestría en Ciberseguridad, cursos libres, certificaciones
- Técnico en Ciberseguridad

Siendo así, se puede afirmar nuevamente que la gran mayoría de instituciones académicas encuestadas si incluyen formación o cursos propios en ciberseguridad, estos datos representan un panorama positivo para la ciberseguridad, ya que este compromiso constituye un aspecto fundamental para cultivar un ecosistema robusto de profesionales capaces de abordar los desafíos emergentes en ciberseguridad.

Respecto a los **convenios con instituciones o empresas para la formación en ciberseguridad**, los resultados de 2023 señalaron que la gran mayoría de instituciones académicas (81,8%) mantenía convenios con instituciones o empresas para la formación en ciberseguridad, contrastado con un 60% para 2024. La reducción del 81,8% al 60% en convenios puede resaltar que hay poca prioridad institucional para la colaboración en ciberseguridad. Lo anterior, podría ser resultado de factores como falta de recursos, cambios estratégicos, entre otros.

No obstante, el 20% de respuestas "desconozco" en 2024 contra el 0% del año anterior puede implicar que los encuestados tienen menos información sobre los convenios institucionales, lo cual puede reflejar problemas de comunicación interna o falta de transparencia en las decisiones estratégicas. Adicionalmente, si bien en el 2023 el 18,2% de los encuestados respondieron que su institución no mantiene conversación con otras instituciones para la formación en ciberseguridad, en la edición 2024 este porcentaje se mantuvo bastante similar incrementando a 20%.

Gráfico 3. Convenios para la formación de Ciberseguridad



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

El informe de 2024 revela una disminución preocupante en la percepción y participación en convenios de colaboración en ciberseguridad, esto pone de relieve la necesidad de reforzar la importancia de la cooperación interinstitucional para abordar los crecientes desafíos del ciberespacio. Además, sería fundamental trabajar en mejorar la comunicación interna y la transparencia de las instituciones para garantizar que estas alianzas sean conocidas y utilizadas de manera efectiva.

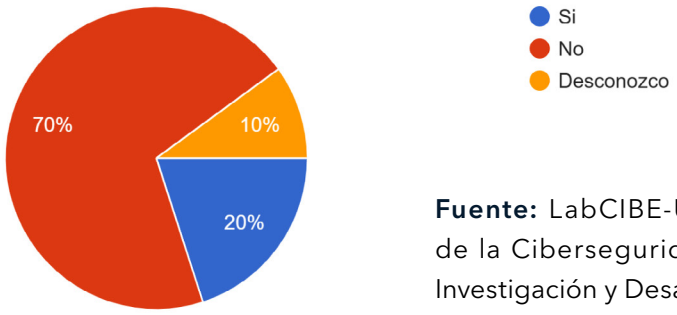
En referencia a la **efectividad de convenios**, en esta edición a fin de complementar el diagnóstico, se realizó una pregunta cualitativa que evalúa no solo la existencia de convenios, sino también su impacto en la formación y la calidad de los programas, los

resultados recopilados indican que un 50% consideran muy efectiva la implementación de convenios, mientras el restante 50% lo considera efectivo, de manera que se concluye que continúa representando un beneficio recíproco entre ambas partes.

En cuanto a la disponibilidad de **presupuesto exclusivo a actividades de investigación y desarrollo en ciberseguridad**, el gráfico 4 evidencia la comparación con las respuestas del año 2023, que frente a la disminución en la participación, en principio existe una drástica reducción en respuestas afirmativas, pues en un año, las instituciones con presupuesto dedicado pasaron del 54,5% al 20%, este cambio podría indicar un cambio en la percepción de las prioridades estratégicas, entre otras posibles causas pueden estar recortes presupuestarios, menor asignación de recursos en áreas de investigación en ciberseguridad.

Por su parte, el aumento del 36,4% al 70% de respuestas negativas refleja una percepción mayor sobre el número de instituciones que no cuentan con financiamiento específico para estas actividades; esto puede ser un indicador del poco protagonismo de la ciberseguridad en la planificación presupuestaria de muchas instituciones. Adicionalmente, el porcentaje de encuestados que no tiene información al respecto se mantuvo relativamente constante (9,1% a 10%). Esto refleja que, aunque haya mayor claridad en las respuestas afirmativas y negativas, sigue habiendo una falta de comunicación interna en algunas instituciones.

Gráfico 4. Presupuesto para I+D en ciberseguridad



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

Los datos de 2024 evidencian una disminución significativa en el apoyo presupuestario para actividades de investigación y desarrollo en ciberseguridad. Este cambio representa un desafío crítico para el desarrollo tecnológico y la preparación ante amenazas cibernéticas en Costa Rica. Es esencial tomar medidas inmediatas para revertir esta tendencia y garantizar que la ciberseguridad siga siendo una prioridad estratégica a nivel nacional.

Un poco en línea con lo anterior, de las instituciones académicas encuestadas, en comparación con el año anterior, se evidencia que la proporción de instituciones que realizaron **investigaciones en ciberseguridad** disminuyó del 54,5% en 2023 al 40% en

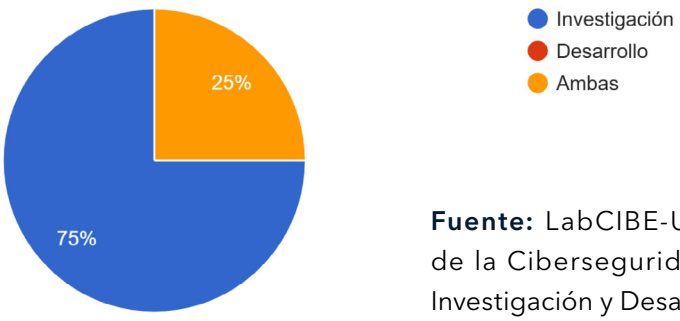
2024, lo que podría ser debido a la disminución de la participación de los encuestado, pero permite enfatizar la pérdida de interés o recursos para impulsar estas actividades. Y sus posibles causas inherentes como posibles recortes presupuestarios, cambios de prioridades estratégicas, y la falta de cultura o sensibilización en materia de seguridad de la información dentro de las instituciones, entre otros factores.

De la misma forma, el incremento del 45,5% en 2023 al 50% de 2024 puede implicar que más instituciones están dejando de involucrarse en investigaciones relacionadas con ciberseguridad. Si bien en 2023 no se registraron respuestas "desconozco", en la presente encuesta se registra un porcentaje de 10%, esto podría indicar que los encuestados no están completamente informados sobre las actividades de investigación dentro de sus propias instituciones.

La disminución de actividad investigativa podría estar vinculada a la falta de financiamiento, lo cual ya se evidenció en la pregunta anterior relacionadas con presupuestos dedicados. Una menor participación en investigaciones puede frenar el avance del conocimiento en ciberseguridad, limitando la capacidad del país para adaptarse a nuevas amenazas y tecnologías emergentes. Se recomienda fomentar colaboraciones interinstitucionales, impulsar alianzas entre instituciones académicas, empresas y el sector público para compartir recursos y capacidades investigativas.

En línea con lo anterior, el 75% de las instituciones enfocadas en ciberseguridad indican que trabajan exclusivamente en investigación, lo cual refleja un enfoque académico o teórico, con menos prioridad en la creación de aplicaciones prácticas o desarrollo de tecnologías en ciberseguridad; exclusivamente el 25% de las instituciones declararon trabajar en ambas áreas, lo cual puede indicar una desconexión entre la investigación teórica y su implementación práctica. Es válido señalar el hecho de que no haya instituciones trabajando exclusivamente en desarrollo, pues resalta un posible vacío en la creación de soluciones aplicadas, herramientas o tecnologías para abordar problemas prácticos en ciberseguridad.

Gráfico 5. Investigación de Ciberseguridad



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

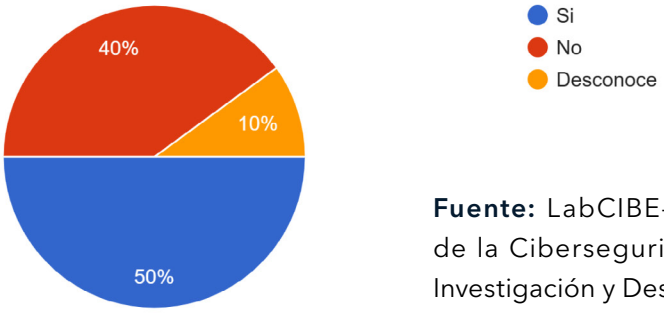
Asimismo, los datos recopilados registran en principio que existen prioridades claras en cuanto a **área específicas de investigación y desarrollo actuales**, pues las áreas de cumplimiento normativo y legal (70%) y respuesta a incidentes (70%) lideran como prioridades institucionales, lo cual refleja una necesidad de mejorar el marco normativo y fortalecer las capacidades reactivas frente a ciberataques. Además, es prudente señalar aquellas áreas emergentes que no han sido priorizadas, tales como IoT (20%), blockchain (10%) y análisis forense (10%) que son menos exploradas, lo que podría representar riesgos no abordados adecuadamente en un entorno tecnológico en constante evolución.

El análisis de las áreas prioritarias en ciberseguridad revela un notable desequilibrio en la distribución de esfuerzos investigativos. Si bien las áreas tradicionales como seguridad de redes y análisis de *malware* mantienen una posición relevante con un 60% de atención cada una, existe una brecha significativa respecto a tecnologías más innovadoras como la inteligencia artificial, que solo alcanza un 40% de interés, o blockchain, que recibe aún menos atención. Particularmente alarmante resulta la ausencia total de investigaciones en sistemas industriales, con un 0% de participación, lo cual genera preocupación considerando su papel crucial en la protección de infraestructuras críticas nacionales.

Adicionalmente, la inversión en investigación sobre ciberseguridad en entornos cloud se mantiene en niveles bajos, con solo un 20% de las instituciones abordando esta área, lo que podría indicar tanto una adopción tardía de estas tecnologías como una carencia de recursos y personal especializado en este campo.
Siendo así, los resultados de 2024 proporcionan una visión clara de las áreas prioritarias en ciberseguridad, pero también evidencian brechas en temas emergentes como IoT, blockchain y sistemas industriales. Para mejorar la preparación ante amenazas futuras, será crucial equilibrar los esfuerzos en áreas tradicionales y emergentes, fomentando la innovación y fortaleciendo las capacidades nacionales en ciberseguridad.

No obstante, en relación a **planes futuros para realizar proyectos de investigación y desarrollo en ciberseguridad**, si bien en 2023, una mayoría significativa (72,7%) de las instituciones señaló que tenían planes futuros en términos de investigación y desarrollo (I+D) en ciberseguridad, y un 27,3% no tenía planes, y ninguna institución indicó desconocer esta información. A diferencia de la encuesta anterior, en 2024, el porcentaje de instituciones con planes futuros disminuyó al 50%, las respuestas negativas ("no") aumentaron significativamente al 40%, y por tanto, 10% indicó desconocer del tema.

Gráfico 6. Planes futuros de investigación y desarrollo en ciberseguridad



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

El análisis de la planificación en investigación y desarrollo en ciberseguridad revela una tendencia preocupante. Se ha observado una significativa disminución, pasando del 72.7% al 50% en las instituciones que reportan tener planes futuros en este campo, lo cual sugiere que hay poca capacidad en las instituciones para desarrollar estrategias de largo plazo en I+D de ciberseguridad. Esta tendencia negativa se ve reforzada por el incremento en las respuestas negativas, que aumentaron del 27.3% al 40%, donde se percibe en 2024 que más instituciones han optado por no invertir o planificar en este ámbito. Mientras que en 2023 todas las instituciones tenían clara su posición respecto a la planificación futura, en 2024 emergió un nuevo segmento del 10% que manifestó desconocer los planes futuros de su organización en materia de ciberseguridad.

El cambio de percepción entre ambos años podría estar relacionado con factores externos como restricciones presupuestarias, cambios de prioridades institucionales o la falta de recursos humanos especializados en ciberseguridad. Sin planes claros, las instituciones podrían enfrentar dificultades para generar soluciones innovadoras y mantener su competitividad en el ámbito de la ciberseguridad.

Por otra parte, en cuanto a las **principales barreras identificadas por las instituciones en términos de investigación y desarrollo en ciberseguridad** se identifica principalmente al financiamiento (100%), en el sentido que todas las instituciones indicaron que la falta de financiamiento es el principal obstáculo para avanzar en I+D en ciberseguridad, seguido de escasez de personal calificado (90%) ya que la falta de talento humano especializado limita significativamente sus capacidades en esta área, en tercer lugar, el acceso a datos/ infraestructuras (50%) y la colaboración público-privada o público-público (40%)

A continuación, un análisis comparativo entre los años anteriores 2023, 2024:

1. El financiamiento como la mayor barrera: la unanimidad en este punto resalta la necesidad crítica de recursos económicos para impulsar proyectos de ciberseguridad. Esto sugiere que las instituciones no cuentan con presupuestos adecuados para implementar iniciativas significativas en esta área.

2. Déficit de personal especializado: la escasez de talento humano calificado indica un vacío en la formación de profesionales con competencias específicas en ciberseguridad, lo cual limita la capacidad de las instituciones para abordar los retos tecnológicos.
3. Limitaciones en infraestructura y datos: el acceso restringido a infraestructura tecnológica y datos relevantes subraya la necesidad de desarrollar entornos más abiertos y colaborativos para facilitar la investigación.
4. Colaboración limitada: aunque no es la barrera principal, la falta de colaboración entre sectores público y privado es un desafío significativo, esto sugiere que las instituciones podrían beneficiarse de alianzas estratégicas para compartir recursos y conocimientos.

De esta manera, los resultados de 2024 revelan que el financiamiento, la escasez de personal calificado y el acceso limitado a infraestructuras son las principales barreras para la investigación y desarrollo en ciberseguridad, si bien bordar estas limitaciones requerirá una estrategia integral que combine inversión, formación de talento y colaboración entre sectores, sin estos esfuerzos, el progreso en ciberseguridad podría verse comprometido, poniendo en riesgo la preparación tecnológica del país.

En lo que concierne a percepción en cuanto a la **relevancia de la investigación y desarrollo en ciberseguridad** en institución académicas, en comparación con el año 2023, se evidencia un aumento en la percepción de máxima importancia (54,5% al 60%) e inclusive en instituciones que consideran la ciberseguridad como "muy importante" refleja una mayor prioridad percibida de este tema en 2024. En adición, se presenta una reducción en el nivel de importancia moderada, la disminución del 27,3% al 20% sugiere que algunas instituciones están fortaleciendo su compromiso con la ciberseguridad al pasar de considerarla "muy importante". Por su parte, la proporción de respuestas neutrales se mantuvo estable (18,2% en 2023 y 20% en 2024), indica que algunas instituciones todavía no perciben la ciberseguridad como un área crítica, pero tampoco la descartan.

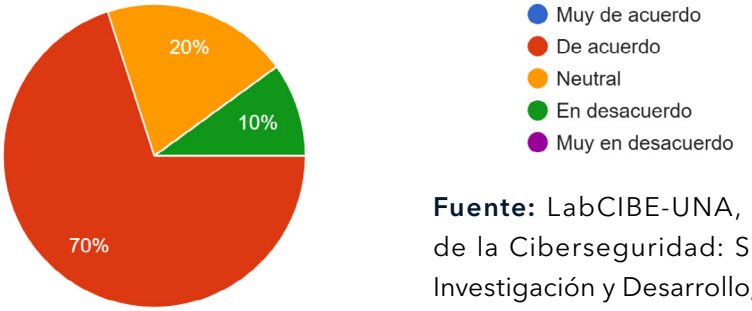
El análisis muestra un aumento en la percepción de la ciberseguridad como "muy importante" entre 2023 y 2024, reflejando un avance en su reconocimiento como una prioridad estratégica. Sin embargo, las respuestas neutrales y la reducción en la categoría "importante" destacan la necesidad de un esfuerzo continuo para involucrar a todas las instituciones en la importancia crítica de la investigación y desarrollo en esta área.

A fin de conocer un poco más la **percepción de los encuestados**, 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."*

De acuerdo a los datos registrados, la mayoría de los encuestados están de acuerdo con la afirmación de que las actividades de I+D en ciberseguridad están mayoritariamente centradas en proyectos de fin de carrera o posgrado, mientras que una quinta parte de los encuestados no tiene una posición definida sobre si estas actividades están limitadas al ámbito descrito, y solo un pequeño porcentaje de los encuestados discrepa, indicando que estas actividades podrían tener un alcance más amplio que el señalado.

Gráfico 7. Percepción sobre afirmación sobre I+D limitante en instituciones académicas



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

De esta manera, estos resultados destacan una percepción mayoritaria de que las actividades de investigación y desarrollo en ciberseguridad en Costa Rica están limitadas a proyectos de fin de carrera o posgrado. Si bien hay ejemplos que podrían indicar lo contrario, hay una amplia percepción de que estas iniciativas solo se dan a través de proyectos de fin de carrera de los programas de posgrado y por lo tanto, existe un faltante de programas de extensión por parte de las instituciones académicas donde se puedan dedicar esfuerzos en investigación y desarrollo en ciberseguridad.

3.2.2 Situación Jurídica de la Ciberseguridad Nacional

La presente sección pretende diagnosticar la situación jurídica de la ciberseguridad nacional desde la perspectiva jurídica, enfocado en aspectos de seguridad cibernética, prevención de incidentes informáticos, capacitación y formación en ciberseguridad, implementación de la inteligencia artificial así como recursos y presupuesto asignados. De manera que, comprende los resultados de la totalidad de los encuestados. A continuación, se presenta una visión detallada sobre la situación jurídica actual de la ciberseguridad en Costa Rica, contemplando comparativamente los resultados del Estado de la Ciberseguridad 2023.

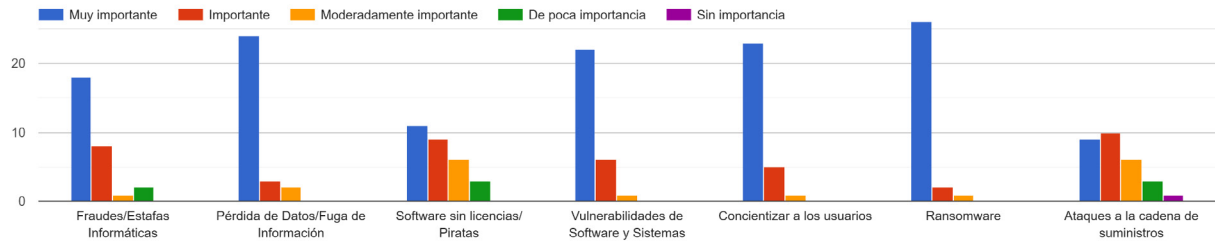
3.2.2.1 Seguridad Cibernética

Respecto a las **mayores preocupaciones** en materia de seguridad cibernética, los resultados determinan que a diferencia de la encuesta anterior, la principal preocupación gira en torno a la presencia de *ransomware* en sus sistemas informáticos, así lo indica en el 89,6% de los encuestados, esto en virtud de que puede implicar la pérdida de acceso a datos esenciales e incluso confidenciales para la organización, y por ende resultando en impactos significativos; en segundo lugar por segundo año comparativo se posiciona la pérdida de datos/ fuga de información con un 82,7%, este resultado refleja una constante preocupación debido al posible impacto a nivel crítico en sus operaciones así como en la imagen de la organización, el experimentar una fuga de información.

En cuanto a la concientización de usuarios, este aspecto experimentó una notable disminución en su nivel de prioridad, pues si bien en esta edición 23 participantes considera relevante este factor, en términos comparativos pasó de posicionarse la mayor preocupación al tercer lugar según los encuestados, lo cual podría significar avances significativos en la cultura de ciberseguridad en las instituciones, el cambio de prioridades organizaciones o inclusive la implementación de nuevas herramientas de identificación de ataques cibernéticos. Seguidamente, muy similar en el caso de vulnerabilidades de *software* y sistemas, 75,86% de los encuestados indicaron que representa una preocupación de moderada importancia.

Si bien más de la mitad de los participantes (62,06%) consideran que los fraudes/ estafas informáticas constituyen una de sus preocupaciones más importantes, este dato es ligeramente menos significativo en comparación con los demás factores, y similar al año anterior continúa posicionándose en una amenaza menos relevante para los participantes. Por su parte, los datos registran que tanto la presencia de *software* sin licencias/piratas como los ataques a la cadena de suministros no representa un factor tan importante, pues únicamente menos de un tercio de los encuestados los consideran como preocupaciones importantes.

Gráfico 8. Preocupaciones en seguridad cibernética



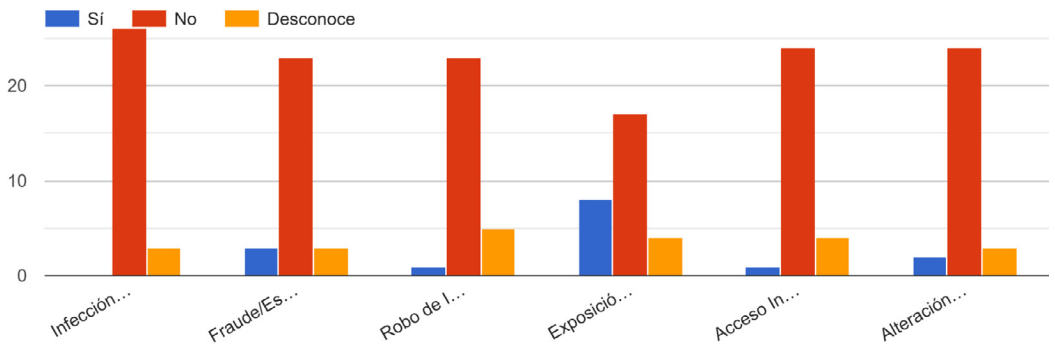
Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

A pesar de que las organizaciones han identificado sus principales preocupaciones en seguridad cibernética, los resultados muestran una discrepancia significativa, pues un alto porcentaje de los encuestados no dispone de un **seguro de ciberseguridad** para protegerse frente a posibles incidentes informáticos, únicamente disponiendo de uno el 13,8%; que si bien del porcentaje que no cuenta con uno, más de 50% se encuentra interesado en adquirirlo, este vació en cuanto a la cobertura frente a un ataque cibernético denota una falta de preparación ante riesgos de esta índole.

No obstante, pese a las constantes inquietudes en torno a incidentes cibernéticos e inclusive ante la ausencia de cobertura en ciberseguridad, la realidad es que los datos registran que tanto en el 2023 como en el 2024 la mayoría de los participantes no han experimentado ataques similares; particularmente, el 86,66% detalla que no han presentado ataques en cuanto a infecciones de *ransomware* (robo/secuestro de información), asimismo, el 82,76% ha indicado que no ha sufrido accesos indebidos a bases de datos ni alteraciones de sitio web.

Por otra parte, en el caso de de fraudes/estafas así como de robos de información para ambos casos el 79,31% ha indicado que de igual manera, no ha sufrido ataques de esta índice, por lo que, se puede deducir que la mayoría de ataques cibernéticos experimentados por la organizaciones se concentran en otras amenazas, inclusive la encuesta permite evidenciar que a mayor cantidad de ataques informáticos a los que se vieron expuestos los participantes se relacionan con exposición de vulnerabilidades (27,58%). Sin embargo, a pesar de experimentar este tipo de incidentes cibernéticos, solo el 6,9% de las organizaciones participantes proceden a **denunciar el ataque** ante el Sistema Judicial, mientras que el 65,6% no procede con el proceso legal y un 27,6% desconoce si se continúa dicho procedimiento. Lamentablemente, esta situación continua y disminuye la visibilidad y respuesta ante amenazas cibernéticas, dificulta la evaluación de incidentes, limitando así no solo la capacidad de respuesta de entes especializados sino también el desarrollo tanto de estrategias puntuales como de medidas preventivas y correctivas.

Gráfico 9 Ataques cibernéticos



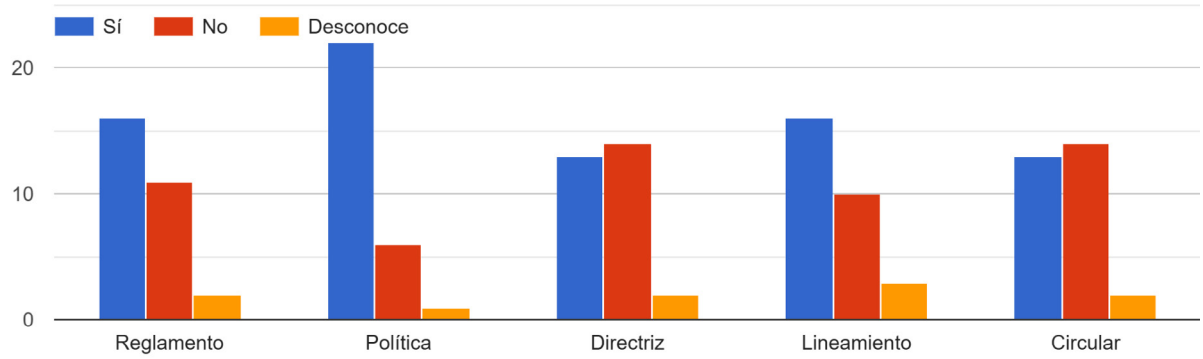
Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

3.2.2.2 Estado de la Ciberseguridad

A fin de contextualizar el estado actual de las instituciones en materia de ciberseguridad es prudente determinar si las organizaciones disponen de algún **protocolo de actuación** ante un incidente informático, en esta edición se evidencia un aumento significativo pues el 82,8% de los participantes confirman contar con procedimientos operativos sólidos de actuación ante ataques informáticos, si bien el 17,2% no dispone de algún procedimiento, este porcentaje ha disminuido en comparación con la encuesta anterior.

En adición a ello, a su vez los datos determinan que las organizaciones disponen ya sea de una política (75,86%), reglamento (55,17%), lineamiento (55,17%), circular (44,82%) o directriz (44,82%) sobre el **uso de los equipos de tecnologías de la información**, lo cual implica la existencia de un marco normativo claro que regula las prácticas internas y promueve un uso responsable y seguro de los recursos tecnológicos del personal de la organización.

Gráfico 10. Establecimiento de normativas internas en materia de tecnologías

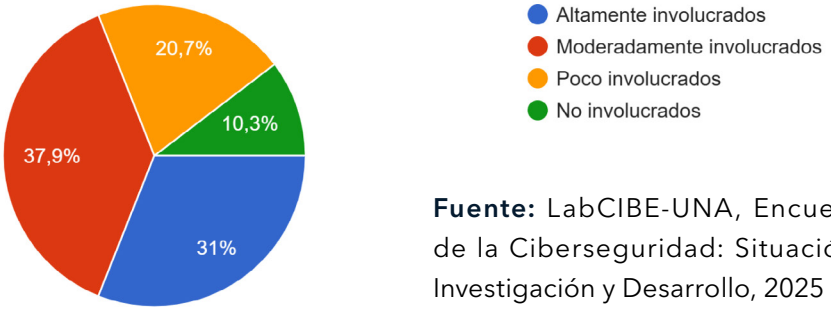


Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

En línea con lo anterior, en cuanto al **nivel de involucramiento de la alta dirección en la decisiones y políticas** en términos de ciberseguridad, se presentan en el gráfico 11 resultados afines a la encuesta 2023, pues se detalla que en el 37,9% de las organizaciones participantes, la alta gerencia se encuentra moderadamente involucrado, mientras que un 31% indica un mayor nivel involucramiento, no obstante, una cifra destacable de un 20,7% implica que la dirección ejecutiva interfiere poco en decisiones de esta índole, y aunque solamente un 10,3% indica que su involucramiento es inexistente o poco significativo, es fundamental que las instituciones participen más activamente en la toma de decisiones de ciberseguridad, no solo para integrar la ciberseguridad en sus operaciones sino también para alinear las estrategias

empresariales con la implementación de nuevas tecnologías y los riesgos que estas implican, particularmente en el entorno tecnológico actual en constante evolución.

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



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

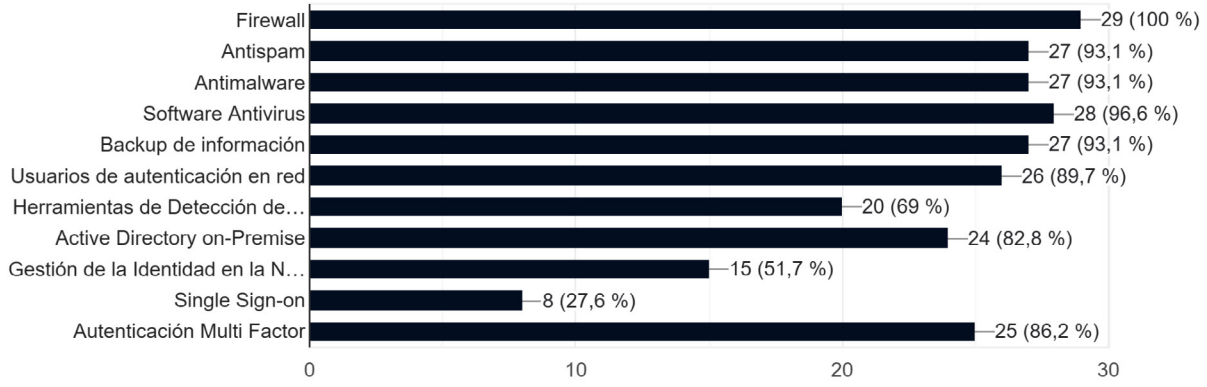
Respecto a la **comunicación de políticas de ciberseguridad**, se evidencia que la principal vía de comunicación al público interno de la organización continúa correspondiendo al envío de correos electrónicos y boletines (96,6%), en el segundo lugar se posicionan las reuniones y capacitaciones (44,8%), y con un porcentaje muy similar (41,4%) por medio del portal interno de la institución, adicionalmente, en menor porcentaje (3,4%) se divulga esta información a través de comunicados informativos con videos.

Un poco en línea con lo anterior, en cuanto a los **mecanismos de actualización sobre tendencias y amenazas cibernéticas**, los datos registran que el 79,3% de las organizaciones encuestadas optan por participar en conferencias/seminarios o en foros de ciberseguridad para mantenerse a la vanguardia en esta materia, seguido de programas de formación/capacitación (69%), mientras que el 31% indica una preferencia por suscripciones a bases de datos especiales como revistas y publicaciones, así como a consultorías externas.

En virtud de que la identificación y evaluación de vulnerabilidades es un componente esencial en la ciberseguridad, es prudente consultar sobre la existencia de **revisiones periódicas del estado de la seguridad** de los sistemas de información en las organizaciones, si bien el 75,9% de los encuestados confirmaron que ejecutan regularmente revisiones, un porcentaje preocupante del 24,1% indica lo contrario.

Por otra parte, según los datos recopilados se evidencia que entre los **principales controles de seguridad cibernética**, la totalidad de las instituciones disponen de sistemas *firewall* (100%), y entre los principales controles de ciberseguridad se encuentran *software* antivirus (96,6%), antispam (93,1%), *antimalware* (93,1%), *backup* de información (93,1%), usuarios de autenticación en red (89,7%) y programas de autenticación multi factor (86,2%).

Gráfico 12. Controles de Seguridad Cibernética

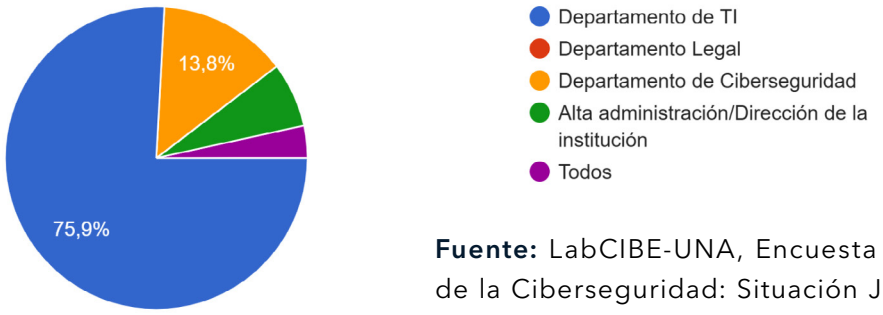


Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

3.2.2.3 Prevención de Incidentes

En la prevención de incidentes cibernéticos, resulta fundamental **determinar en cuál departamento recae este tipo de decisiones**, en comparación con la edición del Estado de la Ciberseguridad, 2023, los datos registran resultados bastante similares, en particular, sugieren que principalmente el departamento de TI son responsables de dichas responsabilidades (75,9%), mientras que un porcentaje menor pero significativo del 13,8% indica que es precisamente el departamento de ciberseguridad, el encargado de aspectos relacionados a esta materia.

Gráfico 13. Departamentos responsables de la prevención incidente cibernéticos

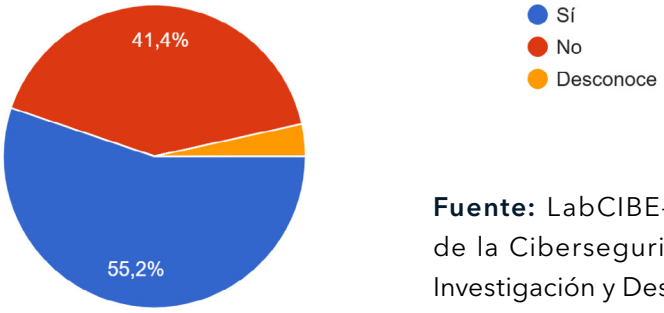


Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

En el panorama actual, donde las amenazas cibernéticas evolucionan constantemente, es de suma relevancia la **identificación de mecanismos de prevención de incidentes** en instituciones públicas y/o privadas, pues constituye un factor esencial para salvaguardar activos críticos, y garantizar tanto la continuidad operativa como la integridad de la organización. De manera que, si bien se evidencia que más de la

mitad de los encuestados (55,2%) efectivamente implementa algún mecanismo de evaluación de riesgo cibernético, un porcentaje significativo (41,4%) aún no ha implementado alguna herramienta de evaluación, esto representa un riesgo para la institución pues no le permite identificar, evaluar y analizar posible incidentes en sus sistemas informáticos.

Gráfico 14. Implementación de mecanismo de evaluación de riesgo cibernético

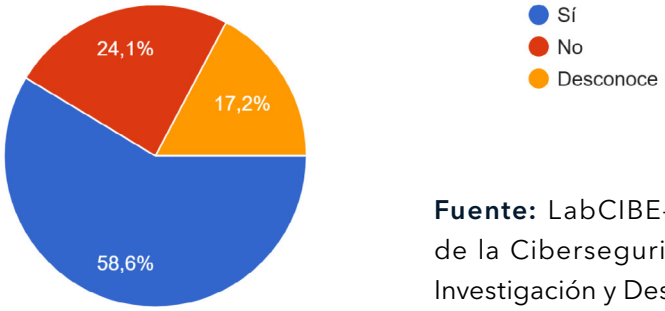


Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

En cuanto al **acceso a la red desde dispositivos personales no gestionados**, los datos señalan que el 75,9% de los participantes restringen este tipo accesos, evidentemente como medida preventiva ante amenazas de índole informático, por tanto, un 24,1% ha detallado que no restringe el acceso de este tipo de dispositivos dentro de la institución, resultados equiparables a la encuesta anterior. Sin embargo, en relación a la **regularización del uso de plataformas digitales** tales como Facebook, Instagram y X, un porcentaje superior al 50% registra que en su organización existe un marco normativo que regula su uso, ya sea por medio de reglamento, protocolo, política, directriz o circular, mientras que un porcentaje relevante del 41,4% la inexistencia de alguna normativa.

Si bien la **protección de datos del cliente** constituye un pilar fundamental de la ciberseguridad a su vez también es un factor esencial en términos jurídicos en cuanto a normativas legales y la prevención de sanciones, siendo así su importancia en el área es justificada y priorizada, la encuesta determinó que el 58,6% de los participantes cuenta con medidas en materia técnica para cumplir la ley de protección de datos del cliente, por ende, un 24,1% no dispone de medidas y un 17,2% desconoce si la organización dispone de este tipo de medidas, pese a que los resultados se asemejan a los del 2023, la realidad es que continúa siendo resultados bastante alarmantes, especialmente para un gobierno en transición tecnológica.

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



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

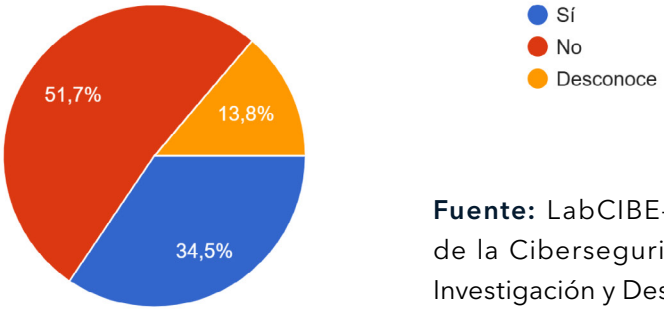
En lo que respecta a la **mayor amenaza que perciben las instituciones**, los datos recopilados determinan que un gran porcentaje de las organizaciones consideran que tanto internamente como externamente se encuentran vulnerables cibernéticamente (62,1%), de manera que, menos significativamente se encuentran aquellas que únicamente perciben que dichas amenazas son únicamente internas (24,1%) o externas (13,8%).

En línea con esto, en cuanto a la **gestión de dispositivos de almacenamiento externo**, se evidencia que principalmente son permitidos pero restringidos (44,8%), seguidamente se detalla que 24,1% no gestiona estos dispositivos formalmente y un 20,7% indica que son permitidos sin restricciones. Sin embargo, estos datos pueden ser un poco alarmantes, particularmente en materia de acceso de datos sensibles, lo cual dificulta el cumplimiento de normativas de seguridad y protección de datos.

Aunado a esto, a diferencia de la edición anterior, en relación al ejecución de **pruebas de *phishing* o simulacros de seguridad**, los datos registran una disminución significativa en medidas de seguridad en, pues la encuesta registra una reducción de 9,7 puntos, ya que los datos recopilados señalan que un 57,7% de las empresas no realizan simulacros de seguridad para evaluar la preparación de los empleados, únicamente el 34,5% procede a realizar este tipo de mecanismos, y un 13,8% desconoce si se realiza este procedimiento, estos resultados sugieren un aumento en la exposición ante ataques informáticos.

Por otra parte, en el caso de aquellas organizaciones que efectivamente realizan pruebas de *phishing* o simulacros de seguridad, se determina principalmente la **frecuencia de este tipo de simulacros** es anualmente con un 80%, mientras que las demás organizaciones lo realizan trimestralmente (20%).

Gráfico 16. Ejecución de simulacros de seguridad

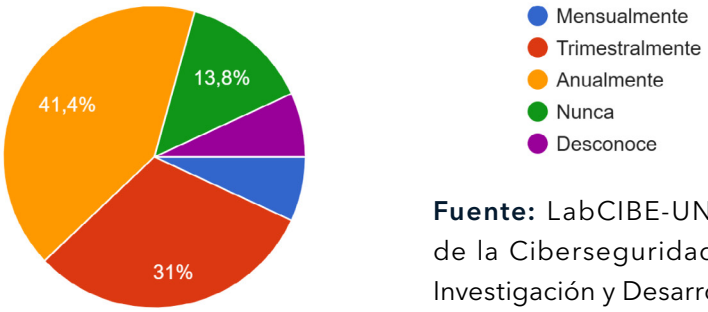


Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

3.2.2.4 Programas de capacitación y/o formación

En virtud de que el escenario actual plantea oportunidades y desafíos para la ciberseguridad, es de suma importancia determinar si la industria cuenta con iniciativas en materia de investigación y desarrollo en ciberseguridad I+D+i, interrogante a la cual similar a la encuesta 2023, la gran mayoría de encuestados (75,9%) ha indicado que no cuentan con iniciativas en esta área, por tanto solamente el 24,1% confirma disponer de programas de este tipo. A pesar de ello, se registra que el 41,4% de los encuestados **participa u organiza conferencias y/o talleres sobre ciberseguridad** al menos una vez al año, un porcentaje igualmente significativo del 31% asiste trimestralmente, y un 13,8% señala que no se realizan ni participan en dichos eventos

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

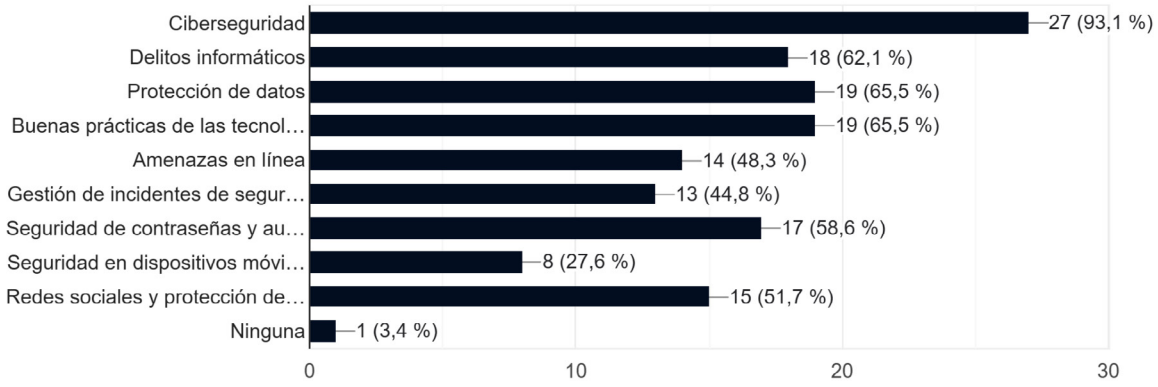


Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

Un poco en línea con lo anterior, los datos evidencian que entre los principales temas de interés en **capacitación o formación** recibidos se determina que el 93,1% registró que el personal de la organización ha recibido capacitaciones sobre ciberseguridad, un 65,5% sobre protección de datos, así como buenas prácticas de las tecnologías de información (TI), seguidamente en delitos informáticos (62,1%), un 58,6% sobre

seguridad de contraseñas y autenticación de doble factor, y 51,7% sobre redes sociales y protección de identidad digital. No obstante, pese a recibir formación en ciberseguridad, a su vez los datos detallan que en un 65,5% de las instituciones estas capacitaciones no constituyen de **carácter obligatorio para el personal**.

Gráfico 18. Temáticas de formación y/o capacitación



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

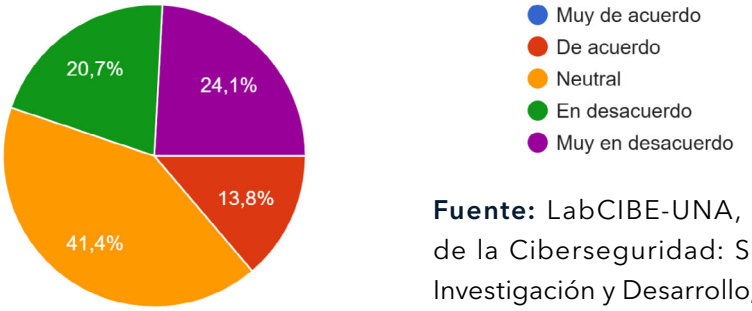
Adicionalmente, se registra que más de la mitad de los encuestados (58,6%) detallan que no disponen de **presupuesto para financiar certificaciones profesionales** en materia de ciberseguridad, únicamente el 34,5%, además, en cuanto a **formación en línea en ciberseguridad**, en su mayoría (72,4%), las organizaciones no ofrecen este tipo de crecimiento profesional.

3.2.2.5 Procedimiento Legal

Respecto a la consulta de procedimientos legales, especialmente enfocado en el **conocimiento de la ley de delitos informáticos**, propiamente los artículos relacionados con la materia en nuestro código penal, se evidencia un resultado constante, pues el 79,3% confirma su conocimiento en la normativa, e inclusive el 82,8% consideran que no es adecuado con respecto a los incidentes informáticos, este dato a su vez se contradice un poco por porcentaje que indica que si la conoce dicha normativa.

La legislación en materia de delitos informáticos constituye un papel fundamental en la prevención de amenazas cibernéticas, si bien su efectividad depende de varios factores, es prudente evaluar la percepción de los encuestados sobre la **efectividad de las leyes y su capacidad para disuadir incidentes cibernéticos**, el 44,8% considera que las sanciones no son suficientes, un 41,4% mantiene un posición neutral al respecto, mientras que 13,8% si considera efectivas las sanciones legales de delitos informáticos.

Gráfico 19. Percepción sobre la efectividad y pertinencia de las sanciones legales por delitos informáticos



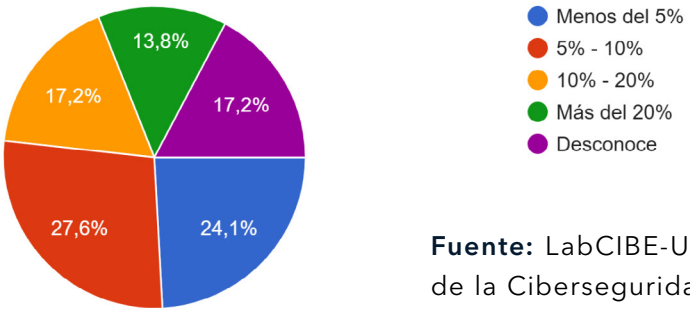
Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

3.2.2.6 Recursos y Presupuesto

A fin de recopilar información sobre el presupuesto asignado y los recursos disponibles con los que dispone la empresa para abordar temas de ciberseguridad en la infraestructura informática de su organización, se asigna una sección específica, ya que la inversión en ciberseguridad es esencial, en el sentido de que se puede traducir en estrategias, medidas preventivas, sistemas de detección e inclusive capacidad de respuesta, así como programas de formación y capacitación.

De manera que, en relación al **porcentaje del presupuesto de TI destinado a ciberseguridad** los resultados en comparación con la encuesta anterior, se distribuyeron en partes muy equitativas, un 27,6% asigna un porcentaje de 5%-10%, el 24,1% destina un porcentaje menor al 5%, mientras que un 17,2% estima un porcentaje entre el 10%-20%, un porcentaje igual de participantes desconoce del monto, y un 13,8% asigna fondos mayores al 20%. Pese a ello, el 82,8% de las organizaciones considera que no es un **presupuesto adecuado** para las necesidades actuales en materia de ciberseguridad.

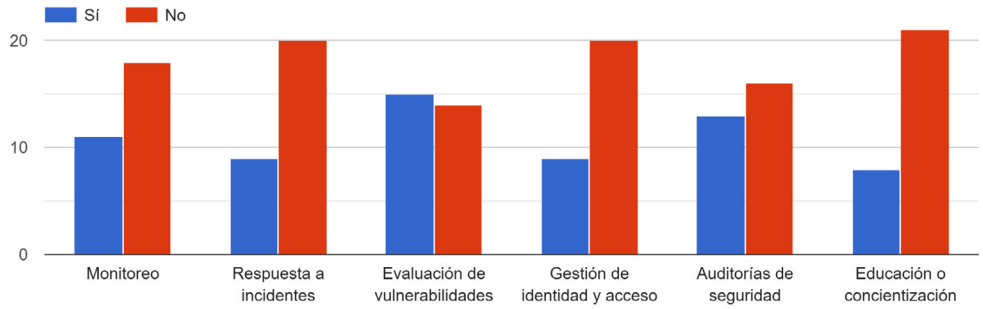
Gráfico 20. Asignación porcentual del presupuesto de TI destinado a ciberseguridad



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

Respecto a la **subcontratación de servicios relacionados con ciberseguridad**, se evidencia que la gran mayoría de empresas no subcontratan o adquieren servicios de esta índole, sin embargo, los datos sugieren que entre aquellos empresas que subcontratan servicios, los principales corresponden a la evaluación de vulnerabilidades, seguido del servicio de auditorías de seguridad y monitoreo, y con menor porcentaje el de respuesta a incidentes, gestión de identidad y acceso y educación o concientización.

Gráfico 21. Subcontratación de Servicios

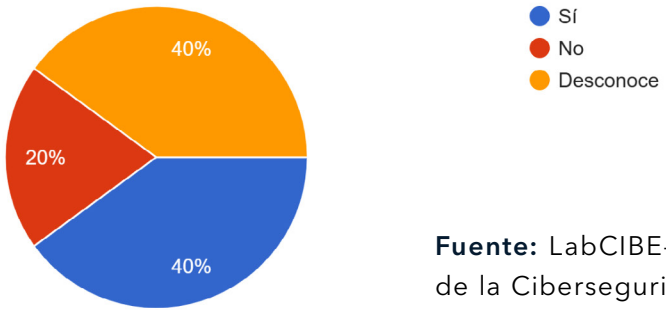


Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

3.2.2.7 Alcance Operativo

En virtud de la relevancia del contexto cibernético, es de relevancia identificar si aquellas organizaciones que desarrollan actividades en mercados extranjeros realizan evaluaciones particulares para cada uno de los mercados donde operan, no solo por riesgos y desafíos específicos de cada entorno en el que operan, sino también para garantizar el cumplimiento jurídico. En primera instancia, únicamente un 17,2% de las organizaciones encuestadas tienen un **alcance operativo** en mercados internacionales, de este rango el 100% opera en América Central, 60% en América del Sur, América del Norte, y Europa respectivamente, y un porcentaje menor de 40% en Asia.

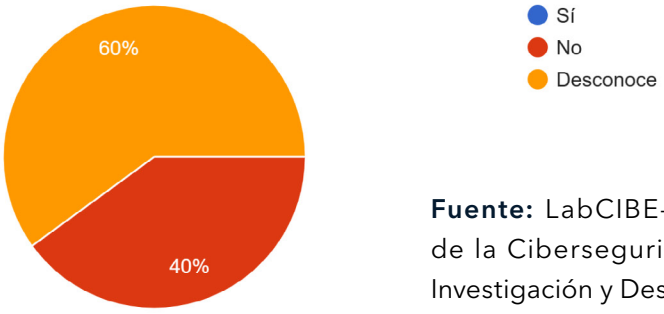
Gráfico 22. Evaluación de riesgos en mercados internacionales



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

De acuerdo con los datos recopilados, en el gráfico 22 se puede evidenciar que la distribución de respuestas sugiere una división bastante equilibrada entre respuestas, pues tanto el 40% de las estas organizaciones confirma **evaluar riesgos cibernéticos** mientras el otro 40% no realiza mecanismos de evaluación en mercados extranjeros. Asimismo, se registra que el 60% de empresas **adaptan sus políticas de ciberseguridad** de acuerdo a la normativa local, mientras que un 20% indica que no lo realiza y un 20% desconoce del procedimiento. Sin embargo, el 100% de los participantes afirma que utilizan una **red privada para la protección de comunicaciones internas y externas**, e inclusive confirmar que no han experimentado ningún ataque cibernético en sus operaciones internacionales.

Gráfico 23. Ataques cibernéticos en mercados extranjeros

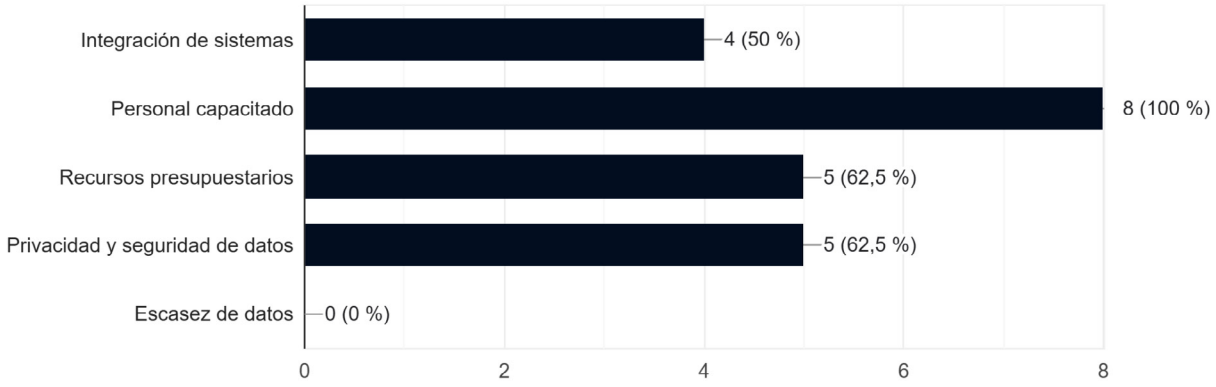


Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2025

3.2.2.8 Inteligencia Artificial

En el contexto actual en donde la inteligencia artificial constituye una tecnología emergente con gran potencial es prudente identificar aquellas organizaciones que han implementado tecnologías de inteligencia artificial en sus operaciones. En esta sección únicamente el 27,6% de los participantes confirmaron utilizar **IA en procesos relacionados con ciberseguridad**, específicamente los resultados indican que principalmente se implementan en la detección de amenazas (87,5%), en segundo lugar en análisis de conductas/comportamiento (62,5%) y en tercer lugar en protección de datos (50%), y en menor porcentaje en investigación así como en respuesta automática de incidentes (37,5%); indiferentemente del área de implementación de IA, el 62,5% de los participantes consideran **efectiva su aplicación**, mientras que el 37,5% mantiene un posición neutral en el tema.

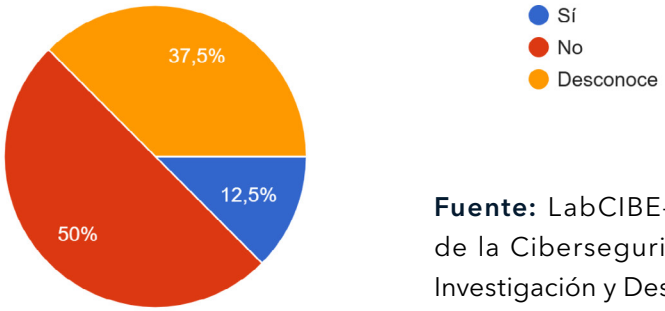
Gráfico 24. Desafíos en la implementación de IA en ciberseguridad



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

Por otra parte, en cuanto a desafíos en la implementación de IA en ciberseguridad, el gráfico 24 evidencia que la mayoría considera como su mayor desafío el personal calificado (100%), seguido de recursos presupuestarios (62,5%) y privacidad y seguridad de datos (62,5), y un 50% considera la integración de sistemas. En línea con esto, un 50% afirma que no disponen de personal calificado, lo cual afirma la escasez de personal capacitado como principal desafío, pues únicamente el 12,5% afirma disponer de personal especializado.

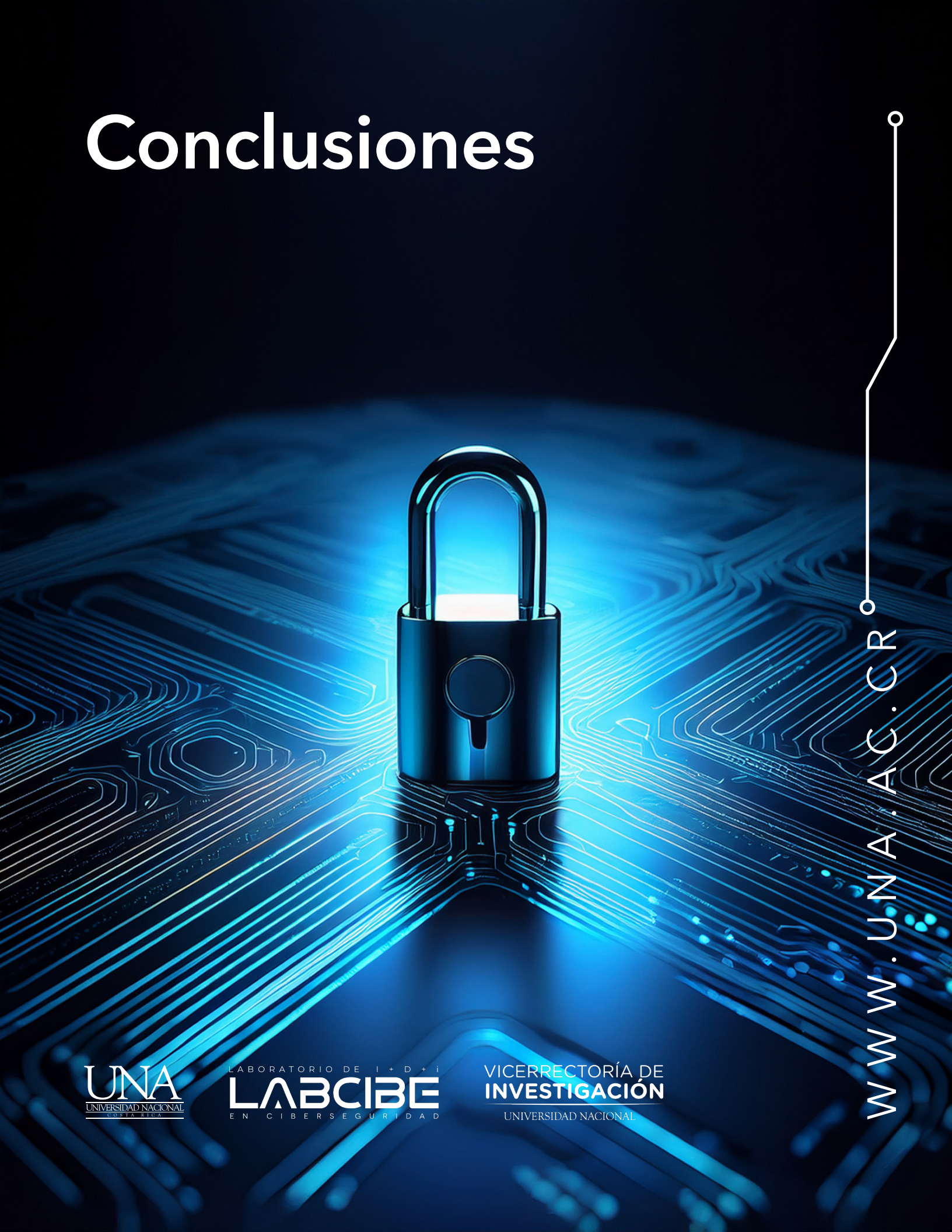
Gráfico 25. Personal capacitado en IA



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

Sin embargo, pese a no contar con personal el 37,5% no invierte ni asigna recursos en la formación y capacitación en inteligencia artificial aplicada a la ciberseguridad, de manera que, sin la capacitación adecuada, el personal no podría implementar, gestionar y optimizar soluciones basadas en IA, y por tanto, la organización queda sin la posibilidad de aprovechar las ventajas competitivas que tecnologías como la IA puede ofrecer.

Conclusiones



UNA UNIVERSIDAD NACIONAL COSTA RICA

LABORATORIO DE I + D + i LABCIBE EN CIBERSEGURIDAD

VICERRECTORÍA DE INVESTIGACIÓN UNIVERSIDAD NACIONAL

WWW.UNA.AC.CR

El análisis detallado del estado actual de la investigación y desarrollo (I+D) en ciberseguridad en Costa Rica revela cambios de percepción sobre el progreso y la evolución de este sector estratégico que podrían no ser tan favorables. Es prudente destacar que los resultados expuestos en este informe no se pueden generalizar, siendo así y considerando esta advertencia y particularmente la disminución en el tamaño de la muestra representativa, se resalta lo siguiente:

En primer lugar, se observa una disminución en la oferta educativa especializada en ciberseguridad. Mientras que en 2023 un impresionante 90,9% de las instituciones educativas ofrecían programas específicos en este campo, en 2024 solo el 70% de las mismas continúan con esta oferta, lo que no es concluyente pues puede deberse a los cambios en la muestra, pero puede reflejar a su vez el poco interés e inversión en la formación de nuevos profesionales en un área crítica para el futuro digital del país. Esta tendencia negativa, a su vez, también es palpable en los convenios de formación, donde la caída de un 81,8% a un 60% en los acuerdos interinstitucionales y empresariales limita las oportunidades de colaboración que son vitales para una formación dinámica y alineada con las necesidades del sector.

Es alarmante aún la situación del financiamiento dedicado a la investigación y desarrollo en ciberseguridad. El presupuesto destinado a estas actividades ha sido percibido como bajo en los últimos 2 años, experimentado 54,5% en 2023 y 20% en 2024, un hecho que plantea dudas sobre la sostenibilidad de la investigación en este campo crucial. Con un 70% de las instituciones reportando la ausencia de un presupuesto específico para I+D en ciberseguridad, se está socavando la capacidad investigativa de las entidades encargadas de enfrentar las crecientes amenazas cibernéticas. Esta falta de recursos se traduce directamente en una baja en la actividad investigativa, estando en un 54,5% al 2024 y un 40% 2024 del total de instituciones que realizan investigaciones en este ámbito, lo que compromete el avance de soluciones innovadoras y eficaces para la protección de los sistemas digitales nacionales.

Un análisis adicional de la distribución de los esfuerzos en investigación y desarrollo, muestra una marcada desconcentración de los recursos. Un 75% de las instituciones se enfocan exclusivamente en investigación, mientras que solo un 25% combina investigación y desarrollo. No se reporta ninguna entidad que se dedique exclusivamente al desarrollo, lo que indica una carencia de enfoques prácticos y aplicados que permitan la implementación de soluciones concretas para los problemas de ciberseguridad en el país. Las prioridades temáticas siguen siendo predominantemente reactivas, con un enfoque principal en cumplimiento normativo y respuesta a incidentes (ambos con un 70% de atención), mientras que áreas emergentes

de gran relevancia como el Internet de las Cosas (IoT), blockchain, análisis forense y sistemas industriales reciben niveles de atención marginal o, en algunos casos, nula.
La planificación futura para I+D en ciberseguridad también refleja señales de alarma. Si bien un 50% de las instituciones contemplan planes de I+D para los próximos años, esta cifra es significativamente más baja que el 72,7% registrado en 2023, lo que refleja la perspectiva de poco protagonismo de la ciberseguridad en planes a futuro. Las barreras identificadas para el desarrollo de estos planes incluyen principalmente la falta de financiamiento (100%), la escasez de personal calificado (90%), y el acceso limitado a datos e infraestructura (50%). Aunque la falta de colaboración público-privada sigue siendo un desafío secundario (40%), su solución podría ser crucial para generar un entorno más colaborativo y eficiente en el desarrollo de soluciones de ciberseguridad.

A pesar de este panorama preocupante, se observa una ligera mejora en la percepción de la importancia de la ciberseguridad, con un aumento del 54,5% al 60% de las entidades que consideran este tema "Muy Importante". Sin embargo, la persistencia de un 20% de opiniones neutrales indica que aún hay una brecha significativa en cuanto a concientización y priorización de la ciberseguridad, especialmente en las instituciones que podrían no considerar el tema como central en su estrategia organizacional.

Un hallazgo relevante es que el 70% de los encuestados en 2024 han señalado que la investigación y el desarrollo en ciberseguridad se concentra principalmente en proyectos de fin de carrera o posgrado, lo que subraya una fuerte dependencia de los niveles más altos de formación académica. Esta concentración en los proyectos académicos de mayor nivel limita la diversidad y expansión de las iniciativas de I+D en ciberseguridad en diferentes etapas educativas, lo que debería ser un punto clave de reflexión para diversificar y ampliar el alcance de las actividades de investigación a nivel nacional.

El panorama de la ciberseguridad en Costa Rica presenta una serie de desafíos y preocupaciones clave que requieren atención inmediata y medidas contundentes para garantizar la protección adecuada frente a las crecientes amenazas cibernéticas. Algunas organizaciones se enfrentan a riesgos significativos, especialmente en relación con el *ransomware*, que ha emergido como la principal preocupación, con un 89,6% de los encuestados considerando este tipo de ataque como el más grave. Este tipo de incidente puede resultar en la pérdida de acceso a datos sensibles y, por tanto, causar daños irreparables a las operaciones de las instituciones. Asimismo, la fuga de información sigue siendo una preocupación relevante, ya que un 82,7% de las organizaciones consideran que la exposición de datos confidenciales tendría consecuencias críticas, tanto en sus operaciones como en su reputación.

En un giro positivo, la concientización de los usuarios sobre los riesgos cibernéticos parece haber mejorado, aunque su prioridad ha disminuido ligeramente en comparación con ediciones anteriores, lo que podría reflejar avances en la cultura organizacional de seguridad cibernética. Sin embargo, la falta de preparación adecuada frente a estos riesgos es evidente, ya que solo el 13,8% de las organizaciones cuentan con un seguro de ciberseguridad, lo que denota una grave vulnerabilidad ante incidentes informáticos. Aunque la mayoría de las organizaciones no han experimentado ataques graves, la falta de cobertura y la escasa denuncia de incidentes cibernéticos dificultan la respuesta ante estos ataques y limitan el aprendizaje colectivo sobre cómo enfrentarlos de manera efectiva.

En cuanto a las políticas y protocolos internos, las organizaciones han logrado avances importantes en la implementación de procedimientos operativos para enfrentar ataques cibernéticos, con un 82,8% de los encuestados confirmando que disponen de protocolos establecidos, sin embargo, un 17,2% de las organizaciones aún carece de estos procedimientos, lo que subraya la necesidad de continuar trabajando en la estandarización de las respuestas ante incidentes cibernéticos. Además, es evidente que la alta dirección de muchas organizaciones aún no está suficientemente involucrada en la toma de decisiones clave sobre ciberseguridad. Aunque el 37,9% de las organizaciones reportan un nivel moderado de participación de la alta gerencia, un 20,7% señalan que la dirección ejecutiva no está suficientemente involucrada en la estrategia de ciberseguridad, lo que indica una desconexión entre los tomadores de decisiones y la seguridad digital de las instituciones.

Asimismo, la formación y capacitación en ciberseguridad siguen siendo áreas de oportunidad. Aunque un 93,1% del personal ha recibido algún tipo de capacitación sobre ciberseguridad, un 65,5% de las organizaciones no hacen estas capacitaciones obligatorias para su personal, lo que limita la efectividad de estas acciones preventivas. Además, la falta de presupuesto destinado a certificaciones profesionales y formación en línea refleja una barrera importante en el desarrollo continuo de habilidades en este ámbito crucial.

En cuanto a la implementación de inteligencia artificial (IA) en las organizaciones, solo un 27,6% de las instituciones utilizan IA para fines relacionados con la ciberseguridad, lo que subraya la necesidad de mejorar la inversión en esta tecnología emergente. La falta de personal capacitado en IA (100% de los encuestados mencionaron este como el principal desafío) y la escasez de recursos presupuestarios limitan el potencial de las organizaciones para aprovechar las ventajas que ofrece la IA en la detección y mitigación de amenazas cibernéticas.

Finalmente, las organizaciones aún enfrentan desafíos en cuanto a la implementación de medidas preventivas y evaluaciones de riesgos. Un 41,4% de las organizaciones no han implementado herramientas de evaluación de riesgos cibernéticos, lo que las deja expuestas a posibles incidentes. La falta de normativas claras sobre el uso de plataformas digitales y el manejo de dispositivos de almacenamiento externo también refleja un área vulnerable en la protección de datos sensibles y la seguridad de las operaciones. Estos vacíos normativos dificultan el cumplimiento de las regulaciones de seguridad y protegen mal los datos personales de los usuarios.

Referencias bibliográficas

Asamblea Legislativa. (2011). *Ley de protección de la persona frente al tratamiento de sus datos personales*. https://www.tse.go.cr/pdf/normativa/leydeprotecciondelapersona.pdf

Asamblea Legislativa de la República de Costa Rica. (24 de Octubre de 2001). *Adición de los artículos 196 bis ("Violación de comunicaciones electrónicas"), 217 bis ("Fraude informático") y 229 bis ("Alteración de datos y sabotaje informático") al Código Penal*.

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

Asamblea Legislativa de la República de Costa Rica. (13 de Octubre de 2005). *Ley de Certificados, Firmas Digitales y Documentos Electrónicos*.

Asamblea Legislativa de la República de Costa Rica. (2008). *Tratado de Libre Comercio entre Norte América, Centroamérica y República Dominicana (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). *Aprobación de la Convención Interamericana sobre Asistencia Mutua en Materia Penal*. http://ministeriopublico.poder-judicial.go.cr/coop-intern/inst-inter/02/18.pdf

Asamblea Legislativa de la República de Costa Rica. (08 de Setiembre de 2011). *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. (05 de Setiembre de 2011). *Ley de protección de la persona frente al tratamiento de sus datos personales*.

Asamblea Legislativa de la República de Costa Rica. (2012). *Reforma de varios artículos y modificación de la sección VIII, denominada delitos informáticos y conexos, del título VII del Código Penal*.

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

Avendaño Rivera, A. (13 de Noviembre de 2012). (R. Lemaitre Picado, Entrevistador)

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

Barquero Elizondo, A. (01 de Noviembre de 2012). (R. Lemaitre Picado, Entrevistador)

Barrantes Sliesarieva, E. G. (2010). *Conceptualización de la Ciberseguridad*. San José: PROSIC.

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

Carvajal Chavarría, J. F. (26 de Octubre de 2012). (R. Lemaitre Picado, Entrevistador)

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 de julio de 1992). *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). *Acuerdo CONASSIF 5-24 (v01 5 agosto 2024)*: Reglamento General de Gobierno y Gestión de la Tecnología de la Información en las entidades financieras. https://www.sugef.fi.cr/normativa/normativa_transversal/documentos/CONASSIF%205-24%20(v01%205%20agosto%202024).pdf

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

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

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

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

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

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*. http://www.firmadigital.go.cr/Info.html

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

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

González Castillo, A. (09 de Noviembre de 2012). (R. Lemaitre Picado, Entrevistador)

Grupo de los Ocho. (Junio de 2010). *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. (26 de mayo de 2011). *Deauville Declaration: Internet*. http://www.g7.utoronto.ca/summit/2011deauville/2011-internet-en.html

Herrera Céspedes, A., & Fonseca Salazar, C. (31 de Octubre de 2012). (R. Lemaitre Picado, Entrevistador)

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

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

International Telecommunications Union. (2007). *GCA Goals*. http://www.itu.int/osg/csd/cybersecurity/gca/goals.html

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

International Telecommunications Union. (2008). *ITU Global cybersecurity Agenda (GCA) High-level experts group (HLEG) Global Strategy Report*. Cybersecurity-gateway.org: http://www.cybersecurity-gateway.org/pdf/global_strategic_report.pdf

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

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

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

International Telecommunications Union. (2010). *ITU Resolution 130*. http://www.itu.int/osg/csd/cybersecurity/WSIS/RESOLUTION_130.pdf

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

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

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

International Telecommunications Union. (2010). *Resolution 69 - Creation of national computer incident response teams, particularly for developing countries and cooperation between them*. http://www.itu.int/osg/csd/intgov/resoultions_2010/resolution69.pdf

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

Lead University. (s.f.). *Técnico Especializado en Ciberseguridad*. Recuperado de 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*. San José: Investigaciones Jurídicas S.A.

Lewis Hernández, E. (30 de Octubre de 2012). (R. Lemaitre Picado, Entrevistador)

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones. (2023). *Estrategia Nacional de Ciberseguridad, Costa Rica 2023-2027*. MICITT

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones. (2023). *Estrategia de Transformación Digital, Costa Rica 2023-2027*. MICITT

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones. (2024). *Estrategia Nacional de Inteligencia Artificial, Costa Rica 2024 – 2027*. MICITT

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

Ministerio de Ciencia y Tecnología. (s.f.). *Firma Digital*. MICITT. http://www.firmadigital.go.cr/DCFD.html

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

Núñez Corrales, S. (01 de Noviembre de 2012). (R. Lemaitre Picado, Entrevistador)

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

Oficina ejecutiva del Presidente de los Estados Unidos de América. (16 de mayo de 2011). *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

Organización de Estados Americanos. (8 de junio de 2004). *Adoption of a comprehensive inter-american strategy to combat threats to cybersecurity: a multidimensional and multidisciplinary approach to creating a culture of cybersecurity*. OEA http://www.oas.org/XXXIVGA/english/docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm

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

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

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

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

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

Presidencia de la República y Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (2024). *Lineamientos para la implementación del proyecto de fortalecimiento de las capacidades en ciberseguridad del país (N° 44487-MICITT)*. http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=102171&nValor3=141134

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

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT). (2022). *Marco Normativo de Gobierno y Gestión de las Tecnologías de Información (TI) en Costa Rica*. https://www.micitt.go.cr/sites/default/files/GobernanzaDigital/MICITT-Marco-Normativo-Gobierno-y-Gestion-TI-v2-2022-firmado-y-sellado.pdf

Poder Ejecutivo y Ministerio de Justicia y Gracia. (21 de Febrero de 2002). *Directrices relativas al empleo ilegal de software en las oficinas gubernamentales y autorización para el 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. (5 de Noviembre de 2004). *Comisión Internet Costa Rica*. http://historico.gaceta.go.cr/pub/2004/11/05/COMP_05_11_2004.pdf

Poder Ejecutivo, Ministerio de Ciencia y Tecnología. (23 de Junio de 2005). *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. (09 de Diciembre de 2010). *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. (13 de Abril de 2012). *Creación del Centro de Respuesta de Incidentes de Seguridad Informática CSIRT-CR*.

Poder Ejecutivo, Ministro de la Presidencia,Ministra de Planificación Nacional y Política Económica. (04 de Octubre de 2010). *Reforma del artículo 1° del Decreto Ejecutivo N° 35139-MP-MIDEPLAN que crea la Comisión Intersectorial de Gobierno Digital*.

Poder Ejecutivo, Ministros de la Presidencia, Planificación Nacional y Política Económica. (06 de Abril de 2009). *Créase la Comisión Interinstitucional de Gobierno Digital*.

Poder Ejecutivo, Ministerio de Salud, Ministro de Gobernación, Policía y Seguridad Pública, Ministerio de la Presidencia, Ministerio de Niñez y Adolescencia. (6 de Mayo de 2004). *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

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

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

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

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

República de Costa Rica. (2023, agosto 25). *Reglamento sobre medidas de ciberseguridad aplicables a los servicios de telecomunicaciones basados en la tecnología de quinta generación móvil (5G) y superiores (N° 44196-MSP-MICITT)*. Diario Oficial La Gaceta. https://www.gaceta.go.cr

Salas Ruiz, J. F. (2010). *El Convenio de Europa sobre ciberdelincuencia*. Programa de la Información y el Conocimiento - Ciberseguridad en Costa Rica. http://www.kerwa.ucr.ac.cr/bitstream/handle/10669/500/libro%20completo%20Ciber.pdf

Superintendencia de Telecomunicaciones. (2011). *SUTEL*. http://sutel.go.cr/Ver/Contenido/que-es-y-funciones-de-la-sutel/41

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

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

Universidad de Costa Rica. Programa de la Sociedad de la Información y el Conocimiento. (2010). *Informe 2010 Hacia la Sociedad de la Información y el Conocimiento*. San José: Impresión Gráfica del Este S.A.

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

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

Universidad Técnica Nacional. (s.f.). *Ingeniería en Software y Tecnologías Informáticas*. UTN. https://www.utn.ac.cr/content/ingenieria-software-tecnologias-informaticas

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

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 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 Castro Carazo. (s.f.). *Técnico en Ciberseguridad 2.0*. https://castrocarazo.info/programas-tecnicos/tecnico-en-ciberseguridad-2-0/?gad_source=1&gclid=CjwKCAiAmrS7BhBJEiwAei59i46I9X6XrCrdmcGiiunMliqwtsqGvrl4U6ID7tFdIeNADdnKxYQxLBoCdh0QAvD_BwE

Universae. (s.f.). *Descubre nuestro 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/#

UNODC. (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

Universidad Nacional (2024). *Estado de la Ciberseguridad en Costa Rica 2023*. Repositorio Institucional UNA. https://repositorio.una.ac.cr/items/edbb7510-bba6-44ef-86ca-8d83cdbbc262

Vega Briceño, E., Lemaitre Picado, R., Villegas Carranza, A., & Solís Cordoncillo, C. M. (2024). *Estado de la Ciberseguridad en Costa Rica 2023*. Universidad Nacional, Costa Rica.