# ESTADO DE LA CIBERSEGURIDAD EN COSTA RICA

# 2023

WWW.UNA.AC.CR

MIEMBRO ACTIVO · Cybersec Cluster · MIEMBRO ACTIVO

LABORATORIO DE I+D+i LABCIBE EN CIBERSEGURIDAD

VICERRECTORÍA DE INVESTIGACIÓN UNIVERSIDAD NACIONAL

UNA UNIVERSIDAD NACIONAL COSTA RICA SEDE REGIONAL CHOROTEGA

UNIVERSIDAD NACIONAL, COSTA RICA
VICERRECTORÍA DE INVESTIGACIÓN
SEDE REGIONAL CHOROTEGA
LABORATORIO DE INVESTIGACIÓN, DESARROLLO E INNOVACIÓN EN CIBERSEGURIDAD

# INVESTIGACIÓN
# ESTADO DE LA CIBERSEGURIDAD EN COSTA RICA 2023

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

Diseño y Diagramación
Ricardo Castro Blanco

Abril 2024
Nicoya, Guanacaste, Costa Rica

005.8
V422e Vega Briceño, Edgar
Estado de la ciberseguridad en Costa Rica / Edgar Vega Briceño, Roberto Lemaitre Picado, Alex Villegas Carranza, Celia María Solís Cordoncillo. – Universidad Nacional, Sede Regional Chorotega, 2024.
1 recurso en línea (99 páginas) : archivo de texto, PDF.
ISBN 978-9968-526-24-1

1. SEGURIDAD (INFORMÁTICA). 2. INTERNET 3. PROTECCIÓN DE DATOS.
I. Lemaitre Picado, Alex, coautor. II. Solís Cordoncillo, Celia María, coautora. III.
Título.

3

# Contenido

# PRESENTACIÓN

La Ciberseguridad, se erige como un pilar fundamental para las sociedades hiperconectadas, siendo un hecho que el ciberespacio es reconocido como un entorno crítico en la gestión de riesgos de la seguridad nacional. Frente a este panorama, es menester capturar una fotografía del estado de la ciberseguridad nacional a través de un instrumento de acceso público.

El informe "Estado de la Ciberseguridad en Costa Rica 2023" expone los principales resultados de la encuesta denominada Estado de la Ciberseguridad 2023: Situación Jurídica, Investigación y Desarrollo. Este informe es realizado por el equipo académico del Laboratorio de Investigación, Desarrollo e Innovación en Ciberseguridad (LabCIBE) de la Sede Regional Chorotega y de la Vicerrectoría de Investigación de la Universidad Nacional (UNA).

El estudio incorpora la dimensión de Investigación, Desarrollo e Innovación (I+D+i), así como la dimensión de marcos regulatorios en Costa Rica, abarcando cuestiones relativas al delito informático y el proceso penal.

El objetivo principal es diagnosticar anualmente la situación de la ciberseguridad en el país y generar resultados, los cuales están dirigidos a distintos actores, incluidos tomadores de decisiones en el sector público y privado, organismos de seguridad nacional, empresas tecnológicas, académicos, investigadores y grupos organizados de la sociedad.

Al proporcionar un diagnóstico sobre la situación actual de la ciberseguridad en el país, el informe pretende ser una herramienta para la formulación de políticas, la planificación estratégica y la implementación de medidas efectivas de prevención y respuesta ante incidentes cibernéticos.

Edgar Vega Briceño
Coordinador LabCIBE

# INTRODUCCIÓN

En el escenario actual, los avances tecnológicos, la interconectividad y la comunicación digital constituyen factores esenciales para la sociedad, a tal magnitud que incluso la dinamizan significativamente, por lo que, en un contexto en donde la tecnología y la comunicación digital dominan, la innovación se presenta como un pilar fundamental, en el sentido que representa una herramienta clave para competir en un mercado altamente competitivo. En consecuencia, la protección de la propiedad intelectual e industrial se convierte no solo en un imperativo estratégico, sino en una obligación legal y ética, ya que aparte de ser una ventaja competitiva exclusiva y temporal, y muy valiosa para el mercado, también cuenta con gran valor comercial, investigativo y de desarrollo.

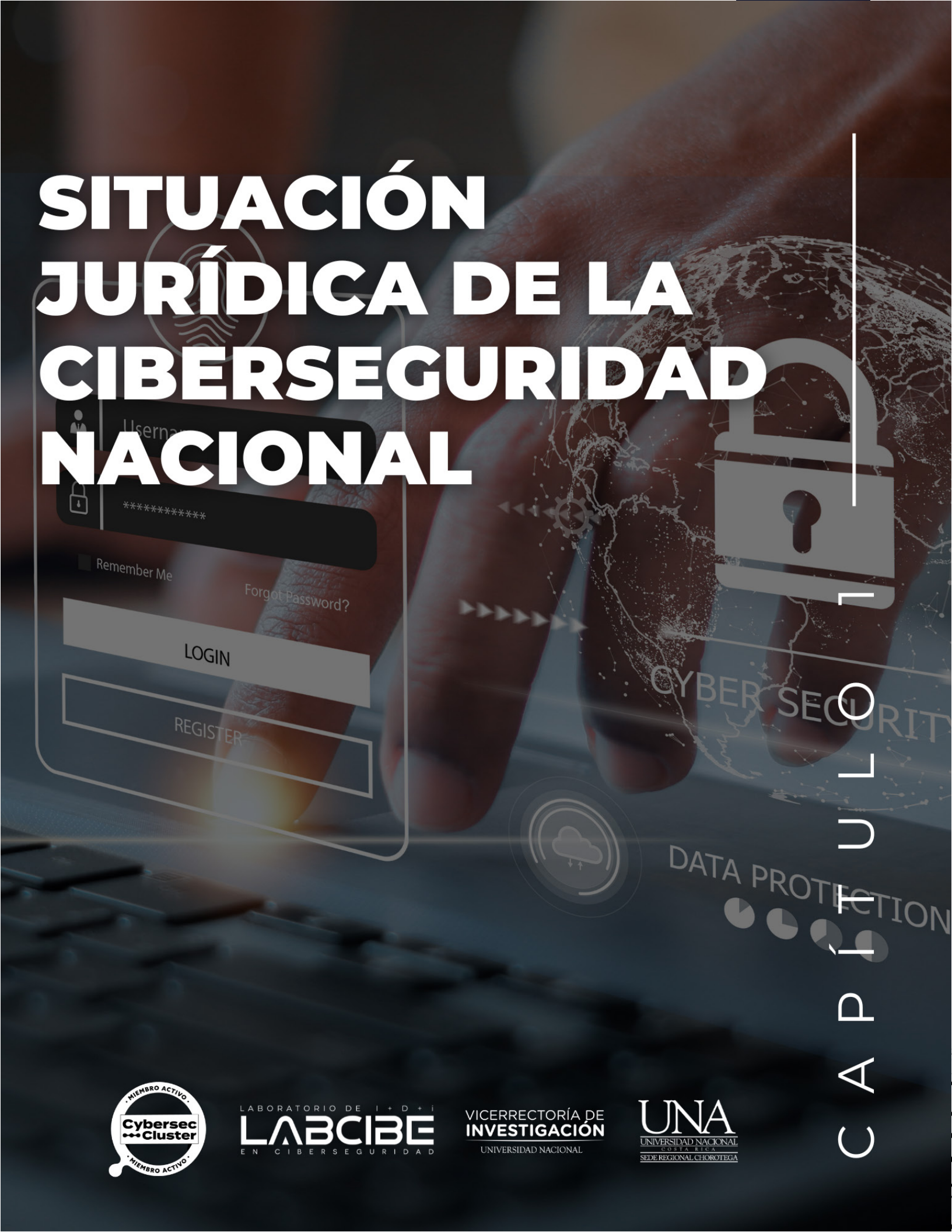
Sin embargo, es innegable que cada adelanto tecnológico a su vez implica retos y desafíos en materia de seguridad, particularmente en el ámbito de las tecnologías de información, en el sentido que, como resultado de la generación, almacenamiento masivo de información y dependencia tecnológica, surgen riesgos, amenazas y vulnerabilidades, lo cual expone a los usuarios, por tanto, es evidente que la ciberseguridad constituye un aspecto de suma relevancia tanto para el sector público y privado.

El presente estudio tiene como objetivo principal determinar anualmente el estado de la ciberseguridad en Costa Rica desde una perspectiva técnica, normativa y de gestión, mediante el diagnóstico estadístico de la situación actual, con el fin de generar conclusiones generales y no particulares, lo cual a su vez permitirá identificar los desafíos presentes y proponer recomendaciones con la intención de fortalecer el entorno de ciberseguridad en el país.

Inicialmente el informe proporciona una conceptualización general de la situación jurídica de la ciberseguridad en el país, abarcando la terminología y el estado regulatorio costarricense; aunado a esto, se examina no solo el papel de las entidades en cuanto a la investigación y desarrollo en el campo de la ciberseguridad, sino también la presencia de la industria en estos esfuerzos. Seguidamente, se presenta el diagnóstico de la situación actual de la ciberseguridad en Costa Rica, basado en los resultados de la encuesta realizada, y culminando con las conclusiones, las cuales no únicamente identifican los desafíos actuales, por el contrario, a su vez ofrecen recomendaciones oportunas para la mejora de la ciberseguridad en el país.

# SITUACIÓN JURÍDICA DE LA CIBERSEGURIDAD NACIONAL

CAPÍTULO 1




MIEMBRO ACTIVO
Cybersec Cluster
MIEMBRO ACTIVO

LABORATORIO DE I+D+i
LABCIBE
EN CIBERSEGURIDAD

VICERRECTORÍA DE INVESTIGACIÓN
UNIVERSIDAD NACIONAL

UNA
UNIVERSIDAD NACIONAL
COSTA RICA
SEDE REGIONAL CHOROTEGA

## 1.1. ¿Qué es la ciberseguridad?

Se debe comprender la ciberseguridad como un componente de la seguridad de la información. La ciberseguridad es la protección de los activos de información haciendo frente a las amenazas a la información procesada, almacenada y transportada por sistemas de información conectados en red.

> La ciberseguridad se ocupa de proteger los activos digitales, es decir, todo lo que abarca el hardware de red, el software y la información que se procesa, se almacena en sistemas aislados o se transporta por entornos de información en red. La seguridad de la información abarca todos los formatos de información; la ciberseguridad se centra únicamente en los activos de información digitales (ISACA, 2021).

Desde el punto de vista técnico la ciberseguridad se enfoca en tres aspectos:

**Confidencialidad:** En principio, su objetivo se centra en garantizar que la información sea exclusivamente accesible a aquellos individuos o sistemas autorizados, por lo que, para mantener la confidencialidad, se utilizan diversas técnicas y herramientas, como:

- **Cifrado de Datos:** Transforma la información en un formato ilegible para cualquier persona que no tenga la clave para descifrarla.

- **Control de Acceso:** Implementa políticas y mecanismos para asegurar que solo los usuarios autorizados puedan acceder a la información. Esto incluye autenticación (verificación de la identidad del usuario) y autorización (permisos para realizar acciones específicas).

- **Redes Privadas Virtuales (VPN):** Ofrecen un canal seguro para la transmisión de datos a través de redes públicas, como Internet.

Integridad: Se refiere a la protección de la información contra alteraciones no autorizadas, ya sean accidentales o malintencionadas, de manera que, las medidas para asegurar la integridad incluyen:

- **Firmas Digitales y Hashes Criptográficos:** Estas tecnologías verifican que el contenido de un mensaje o archivo no ha sido alterado desde su creación.
- **Control de Versiones:** Permite rastrear cambios en documentos o sistemas para identificar alteraciones no autorizadas.

**Derechos de Acceso y Auditorías:** Restringir quién puede modificar información y llevar un registro de cuándo y cómo se hicieron los cambios.

**Disponibilidad:** Asegura que la información y los recursos del sistema estén disponibles para los usuarios legítimos cuando lo necesiten, para ello, se implementan medidas como:

- **Redundancia de Datos y Sistemas:** Copias de seguridad y sistemas duplicados que pueden entrar en funcionamiento en caso de fallos.
- **Protección contra Ataques de Denegación de Servicio (DDoS):** Medidas para prevenir o mitigar los ataques que buscan sobrecargar los recursos del sistema, haciéndolos inaccesibles.
- **Mantenimiento y Actualizaciones:** Asegurar que los sistemas estén actualizados y en buen funcionamiento para prevenir interrupciones.

Siendo así, estos tres pilares de la ciberseguridad trabajan conjuntamente para crear un entorno seguro y confiable. La confidencialidad evita el acceso no autorizado, la integridad asegura que los datos no se alteren de manera indebida, y la disponibilidad garantiza el acceso continuo a la información para aquellos que lo requieran, juntos, forman la base de una estrategia de ciberseguridad efectiva.

### 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 Estado Regulatorio de la Ciberseguridad en Costa Rica

En los últimos años, el marco jurídico correspondiente a la ciberseguridad en el país ha presentado un desarrollo bastante amplio, esto como resultado del crecimiento en las conexiones de internet y el aumento de delitos cometidos por medios informáticos principalmente en materia de estafas informáticas.

Dicho crecimiento de delitos informáticos se puede observar en las estadísticas del Organismo de Investigación Judicial (OIJ), sobre los delitos informáticos ocurridos en el país del 2018 a 2022 y a setiembre 2023.

**Cuadro 1: Delitos informáticos a nivel nacional por mes y año en el período comprendido entre enero de 2018 a setiembre de 2023**

| MES | AÑO | | | | | | TOTAL |
|---|---|---|---|---|---|---|---|
| | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 | |
| ENERO | 119 | 172 | 157 | 215 | 354 | 300 | 1317 |
| FEBRERO | 118 | 160 | 150 | 216 | 672 | 409 | 1725 |
| MARZO | 122 | 189 | 143 | 218 | 1279 | 295 | 2246 |
| ABRIL | 137 | 162 | 180 | 177 | 411 | 319 | 1386 |
| MAYO | 123 | 201 | 262 | 197 | 338 | 408 | 1529 |
| JUNIO | 160 | 191 | 243 | 185 | 251 | 439 | 1469 |
| JULIO | 158 | 245 | 229 | 251 | 260 | 797 | 1940 |
| AGOSTO | 123 | 198 | 194 | 221 | 259 | 475 | 1470 |
| SETIEMBRE | 139 | 172 | 231 | 357 | 283 | 411 | 1593 |
| OCTUBRE | 145 | 130 | 202 | 283 | 248 | | 1008 |
| NOVIEMBRE | 154 | 146 | 194 | 280 | 428 | | 1202 |
| DICIEMBRE | 161 | 144 | 219 | 286 | 374 | | 1184 |
| **TOTAL** | **1659** | **2110** | **2404** | **2886** | **5157** | **3853** | **18069** |

**Fuente: Unidad de Análisis Criminal OIJ**.

**Cuadro 2 Delitos Informáticos a nivel nacional por tipo de delito y año. Enero 2018 - diciembre 2023**

| TIPO DE DELITO | AÑO | | | | | | TOTAL |
|---|---|---|---|---|---|---|---|
| | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 | |
| ESTAFA INFORMÁTICA | 404 | 653 | 940 | 939 | 3124 | 2266 | 8326 |
| SUPLANTACIÓN DE IDENTIDAD | 394 | 635 | 793 | 1032 | 830 | 772 | 4456 |
| OTRO O INDETERMINADO | 520 | 488 | 139 | 219 | 212 | 408 | 1986 |
| DIFUSIÓN DE INFORMACIÓN FALSA | 50 | 104 | 120 | 162 | 220 | 126 | 782 |
| SUPLANTACIÓN DE PÁGINAS ELECTRÓNICAS | 88 | 33 | 37 | 107 | 287 | 57 | 609 |
| ESPIONAJE INFORMÁTICO | 34 | 51 | 123 | 132 | 137 | 104 | 581 |
| FACILITACIÓN DE DELITO INFORMÁTICO | 72 | 48 | 51 | 106 | 167 | 39 | 483 |
| SEDUCCIÓN O ENCUENTRO CON MENORES POR MEDIO ELECTRÓNICOS | 54 | 55 | 52 | 65 | 84 | 39 | 349 |
| INSTALACIÓN O PROPAGANDA DE PROGRAMAS INFORMÁTICOS MALICIOSOS | 5 | 8 | 90 | 76 | 50 | 13 | 242 |
| SABOTAJE INFORMÁTICO | 24 | 20 | 34 | 28 | 26 | 22 | 154 |
| DAÑO INFORMÁTICO | 14 | 15 | 25 | 20 | 20 | 7 | 101 |
| **TOTAL** | **1659** | **2110** | **2404** | **2886** | **5157** | **3853** | **18069** |

**Fuente: Unidad de Análisis Criminal OIJ**.

No obstante, pese al gran desarrollo jurídico en materia de ciberseguridad, 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

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

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

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

En su Artículo 1º, 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 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

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 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

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.º 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.

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

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 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.

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

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, 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

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 1º-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 3º—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 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

El "Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR)" fue establecido en 2012 por el decreto Nº 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 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

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.
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.

Esta directriz representa un esfuerzo significativo para mejorar la seguridad informática en las instituciones públicas de Costa Rica, promoviendo la adopción de prácticas de ciberseguridad más robustas y coordinadas.

**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"**

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, por 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.

### 1.2.2.7. Directriz N° 051-MTSS-MICITT “Implementación de sitios web accesibles en el sector público costarricense”

La Directriz N° 051-MTSS-MICITT, subraya el compromiso del país con la igualdad de oportunidades y la accesibilidad para personas con discapacidad, integrando en su estrategia la promoción de tecnologías accesibles y la extensión de los beneficios de las telecomunicaciones a toda la ciudadanía. Esta iniciativa se alinea con diversas leyes, resoluciones y acuerdos tanto nacionales como internacionales, y se fundamenta en la idea de que las Tecnologías de Información y Comunicación (TIC) son clave para fomentar la igualdad y facilitar una vida más independiente para las personas con discapacidad, contribuyendo a erradicar la segregación y discriminación.

Además, se busca garantizar la accesibilidad a los sitios web de las entidades públicas, promoviendo el acceso universal a la información y las comunicaciones y asegurando la inclusión digital, el objetivo es que todas las entidades del Sector Público se adhieran obligatoriamente a los criterios de accesibilidad para sitios web y plataformas digitales establecidos en la norma WCAG 2.1 “Pautas de Accesibilidad para el Contenido Web”. Esto implica adaptar sus formatos para hacerlos más accesibles y adecuados a las necesidades de las personas con discapacidad, sin incurrir en costos adicionales.

Esta directriz facilita el derecho de las personas con discapacidad a acceder a la información y amplía el alcance de la información pública. Además, insta a las instituciones públicas a promover acciones de sensibilización, divulgación, educación y formación en el ámbito de la accesibilidad. Los cambios y modificaciones deben realizarse de manera progresiva según los criterios de la norma WCAG 2.1, priorizando áreas como la educación, lo social y la salud.

Aunque la directriz es obligatoria para el sector público de primer nivel, establece tres estándares de accesibilidad: el nivel A (mínimo), que debe implementarse en un período no mayor a tres años; el nivel AA, con un plazo máximo de seis años; y el nivel AAA, que no tiene plazo establecido, pero es considerado el óptimo.

### 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

El decreto N.º 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 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

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.

**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 a la información de la Estrategia Nacional de Ciberseguridad 2023-2027**

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.

# INVESTIGACIÓN Y DESARROLLO DE LA CIBERSEGURIDAD

CAPÍTULO 2

MIEMBRO ACTIVO · Cybersec Cluster · MIEMBRO ACTIVO

LABORATORIO DE I+D+i LABCIBE EN CIBERSEGURIDAD

VICERRECTORÍA DE INVESTIGACIÓN UNIVERSIDAD NACIONAL

UNA UNIVERSIDAD NACIONAL COSTA RICA SEDE REGIONAL CHOROTEGA

# CAPÍTULO II: INVESTIGACIÓN Y DESARROLLO DE LA CIBERSEGURIDAD

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)

Similar a la UCR, la UNA no ofrece un programa específico de ciberseguridad. Sin embargo, su programa de Ingeniería en Sistemas de Información de manera optativa incluye cursos en este campo. (UNA, s.f.).

#### 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 (Universidad Cenfotec, s.f.).

#### 2.3.2.2. Universidad Latina de Costa Rica

Esta universidad ofrece una Licenciatura en Seguridad Informática y un Técnico en Ciberseguridad (Universidad Latina de Costa Rica, s.f.).

#### 2.3.2.3. Universidad Fidélitas

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

#### 3.2.2.4. Lead University

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

#### 3.2.2.5. Universidad La Salle

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

### 3.2.2.6. 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)

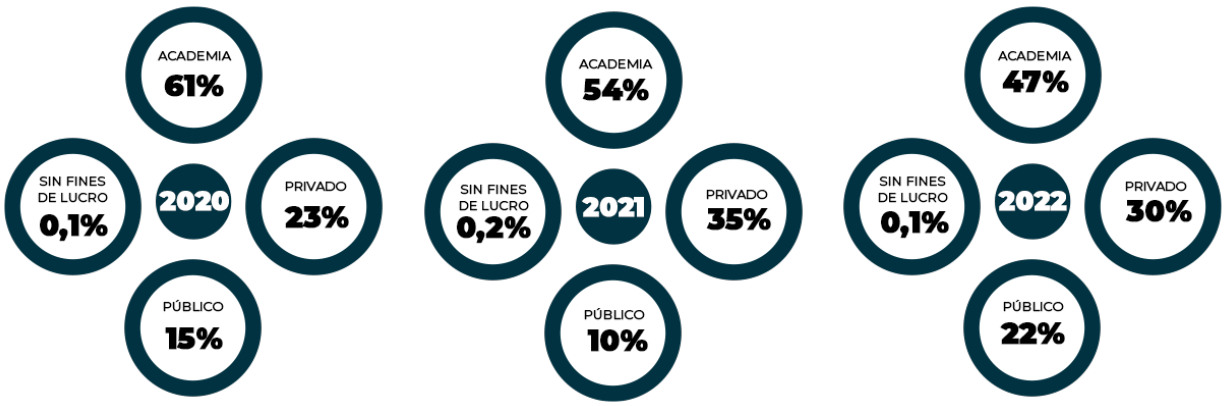
Es evidente que las universidades privadas, a través de estos programas, contribuyen significativamente a la formación de profesionales capacitados y especializados, capaces de afrontar los desafíos de seguridad digital en diversos sectores.

## 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 (TICs); 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.

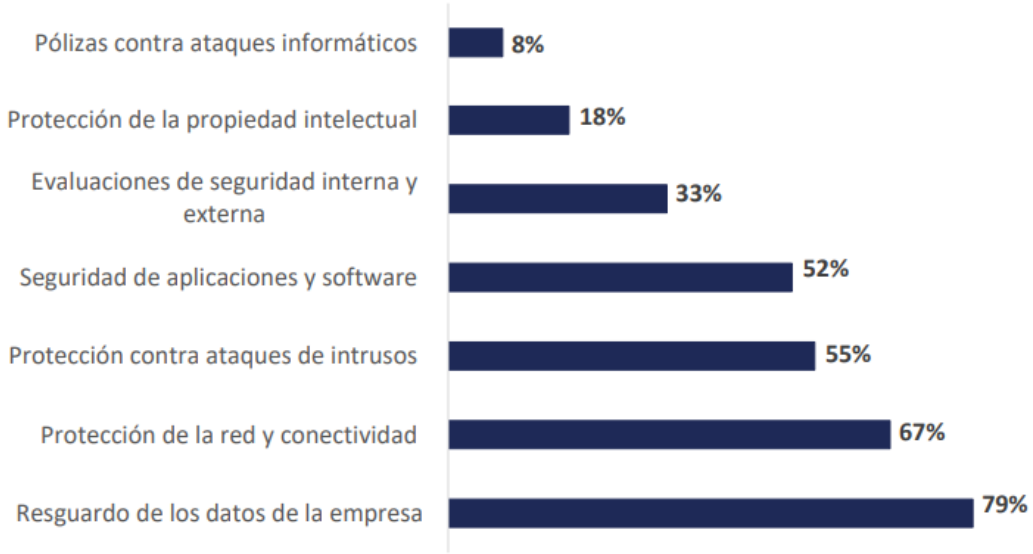
**Figura 1 Distribución de Investigación y Desarrollo según sector**




**Fuente: Informe de Indicadores Nacionales de Ciencia, Tecnología e Innovación en Costa Rica correspondiente al año 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**



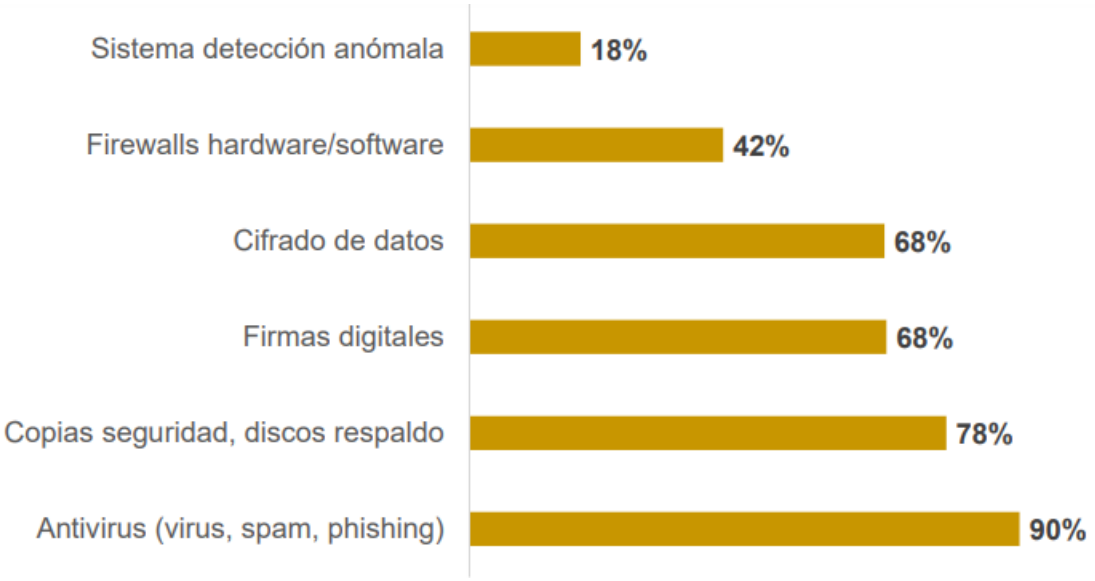

**Fuente: Informe de Indicadores Nacionales de Ciencia, Tecnología e Innovación en Costa Rica correspondiente al año 2022.**

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: Informe de Indicadores Nacionales de Ciencia, Tecnología e Innovación en Costa Rica correspondiente al año 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 otorgaran al completar la carrera.

**5. Análisis comparativo:** Debe presentarse una comparación de la propuesta curricular con respecto a otras universidad estatales o internacionales.

**6. Director de carrera:** Presenta carta debidamente firmada por la persona propuesta como Director de carrera en la que consigne expresamente la aceptación al respectivo cargo por un plazo mínimo de un año.

**7. Infraestructura:** La institución debe contar con las instalaciones adecuadas, laboratorios, recursos bibliográficos y tecnológicos para soportar la enseñanza y el aprendizaje de calidad.

**8. Regulaciones y Cumplimiento:** Presentar el certificado del permiso de autorización emitido por la Dirección de Equipamiento e Infraestructura (MEP), donde se especifique la oferta académica autorizada, la nueva carrera a impartir y capacidad locativa. Asimismo, permiso sanitario de funcionamiento del Ministerio de Salud, certificado de aprobación del Consejo de Salud Ocupacional, registro de propiedad de las instalaciones físicas, o bien, la copia auténtica del contrato de arrendamiento firmado por el representante legal. Finalmente, el certificado de la patente municipal correspondiente. Son una serie de permisos y autorizaciones que se deben obtener de diferentes entidades. Cada uno de estos pasos puede tener sus propios requisitos y tiempos de espera.

**9. Aspectos Financieros:** Establecer tarifas, presenta las tarifas para ser aprobadas por el órgano competente de conformidad con la nueva metodología.

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

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

**2. Modelos pedagógicos virtuales:** La universidad debe presentar el modelo pedagógico que guiará la carrera.

**3. Requisitos básicos Administración Virtual:** Deben describirse varios aspectos, como la infraestructura, la plataforma tecnológica, la estructura de apoyo administrativo, y los procedimientos relacionados con la comunicación.

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

**Figura 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 3

MIEMBRO ACTIVO · Cybersec Cluster · MIEMBRO ACTIVO

LABORATORIO DE I+D+i LABCIBE EN CIBERSEGURIDAD

VICERRECTORÍA DE INVESTIGACIÓN UNIVERSIDAD NACIONAL

UNA UNIVERSIDAD NACIONAL COSTA RICA SEDE REGIONAL CHOROTEGA

# CAPÍTULO III: DIAGNÓSTICO DE LA SITUACIÓN DE LA CIBERSEGURIDAD EN COSTA RICA

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 generar conclusiones generales y no particulares, esto a fin de identificar los actuales desafíos y proponer recomendaciones para fortalecer 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 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.

**Preguntas específicas sobre sobre el estado de I+D :**

1. ¿Ofrece su institución programas de formación o cursos específicos en Ciberseguridad?
2. ¿Mantiene su institución convenios con otras instituciones o empresas para la formación en ciberseguridad?
3. ¿Cuenta su institución con un presupuesto dedicado a actividades de investigación y desarrollo en Ciberseguridad?
4. En el último año, ¿Se han llevado a cabo investigaciones relacionadas a algún área de la ciberseguridad en su institución?
5. ¿Cuenta su organización con planes futuros en términos de investigación y desarrollo en Ciberseguridad?
6. ¿Qué nivel de importancia considera que tiene la investigación y desarrollo en ciberseguridad en su institución?
7. ¿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?
2. ¿Ha sufrido alguno de los siguientes ataques en 2023?
3. 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**

4. ¿En su institución cuentan con algún protocolo de actuación ante un incidente en sus sistemas de información?
5. ¿En su institución se cuenta con algún reglamento, política, circular o directriz sobre el uso de los equipos de tecnologías de la información?
6. ¿En qué medida se involucra la alta dirección en las decisiones y políticas de ciberseguridad?
7. ¿Cómo se comunica la política de ciberseguridad y las mejores prácticas a los empleados?

8. ¿Existen revisiones periódicas del estado de la seguridad de los sistemas de información en su institución?
9. De los siguientes controles de seguridad cibernética ¿De cuáles dispone la empresa?

**Prevención de Incidentes**

10. ¿En qué puesto o departamento recae la responsabilidad de prevenir los incidentes informáticos en su institución?
11. ¿En su institución se implementa algún mecanismo de evaluación de riesgo cibernético?
12. ¿Se restringe en su empresa el acceso a la red desde dispositivos personales no gestionados?
13. ¿Existe algún reglamento, protocolo, política, directriz o circular donde se regule el uso de las Redes Sociales como Facebook, Twitter, Instagram, o alguna similar?
14. ¿La institución cuenta con medidas en materia técnica para cumplir la ley de protección de datos del cliente?
15. ¿Dónde considera que la mayor amenaza de ciberseguridad para su empresa/institución se origina?
16. ¿Se realizan pruebas de phishing o simulacros de seguridad para evaluar la preparación de los empleados?
17. ¿Qué tan frecuente son este tipo de simulacros?

**Programas de capacitación y/o formación**

18. ¿La organización cuenta con iniciativas en materia de investigación y desarrollo en ciberseguridad I+D+i (investigación, desarrollo e innovación)
19. ¿Con qué frecuencia la organización participa u organiza eventos como conferencias o talleres sobre ciberseguridad?
20. ¿En cuáles de los siguientes temas ha recibido capacitación o formación el personal de su institución?

**Procedimiento Legal**

21. ¿Está familiarizado con la ley de delitos informáticos (Código Penal de Costa Rica)?
22. ¿Cree que esta ley cubre adecuadamente los incidentes informáticos en Costa Rica?

**Recursos y Presupuesto**

23. ¿Qué porcentaje del presupuesto de TI se destina a ciberseguridad?
24. ¿Considera que este presupuesto es adecuado para las necesidades de ciberseguridad de su institución?
25. De la siguiente lista ¿La empresa subcontrata algún servicio relacionado con ciberseguridad?

**Alcance Operativo**

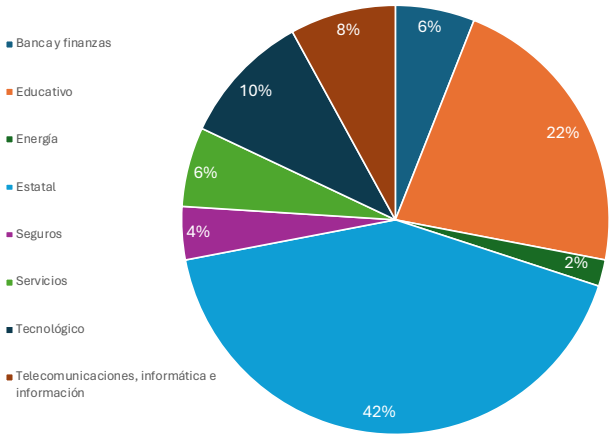
26. ¿Su empresa desarrolla actividades en mercados internacionales?
27. ¿En qué áreas geográficas a nivel mundial tiene presencia o realiza operaciones la organización?
28. ¿Ha evaluado los riesgos de ciberseguridad específicos para esos mercados?
29. ¿La empresa utiliza alguna red privada virtual (VPN) o tecnologías de seguridad similares para proteger las comunicaciones de manera interna y externamente?

## 3.2. Resultados

A continuación, se presentan los resultados obtenidos en esta encuesta, en la cual se recopilaron 50 respuestas de la variedad de actores invitados, proporcionando información relevante sobre el sector en donde desarrollan actividades. Se puede observar que los datos porcentuales revelan una distribución significativa entre los diversos sectores representados, en principio el sector estatal representa un 42%, indicando un alto grado de participación e interés por parte de instituciones públicas gubernamentales en contribuir con la determinación estadística del estado de situación de la ciberseguridad en Costa Rica, asimismo, los datos señalan una participación de un 22% por parte del sector educativo, sugiriendo un compromiso activo por parte de la academia en temas relacionados con la I+D+i.

Seguidamente, un 10% de la información recopilada corresponde al sector tecnológico, mientras que se observa una contribución de un 8% el sector relativo a las telecomunicaciones, informática e información, por su parte, sectores como servicios, banca y finanzas, así como seguros, muestran una participación un poco menos significativo, con un 6% de participación en las encuestas. Aunado a esto, el sector energético representa únicamente un 2% de las encuestas, y un porcentaje menor supone otros sectores no especificados.

**Gráfico 1 Distribución de resultados por sector**




**Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2023.**

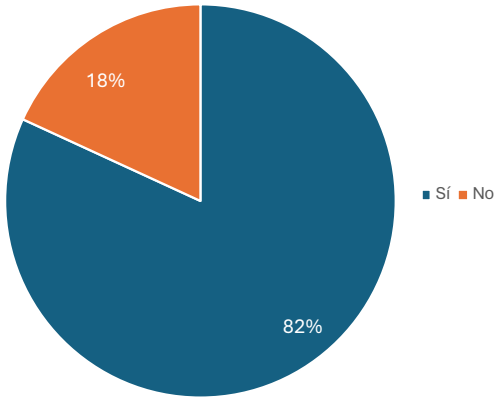
### 3.2.1. Estado de la Investigación y Desarrollo en Ciberseguridad

La presente sección se centra específicamente en la investigación y desarrollo de la ciberseguridad en instituciones académicas costarricenses, de manera que, pretende recopilar información sobre la existencia de iniciativas y/o programas que estimulan la investigación y desarrollo en el área de la ciberseguridad, razón por la cual únicamente comprende el 22% 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, un 90,9% de los participantes señalan que en su institución se ofrecen opciones de educación continua en este ámbito, por tanto, se puede afirmar que la gran mayoría de instituciones académicas si incluyen formación o cursos propios en ciberseguridad, ya que solamente un 9,1% indica lo contrario; siendo así, 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.

Asimismo, los resultados señalan que la gran mayoría de instituciones académicas (81,8%) mantienen convenios con instituciones o empresas para la formación en ciberseguridad, aspecto que representa un beneficio recíproco entre ambas partes, pues facilita el acceso a recursos y conocimientos, fortalece el desarrollo de habilidades y destrezas en ciberseguridad e inclusive aumentar el alcance de proyectos de investigación en conjunto. Esto subraya la importancia de la integración entre el sector educativo y el industrial, en el sentido que, esta sinergia es esencial para la aplicación práctica de conocimientos teóricos y para mantener a los futuros profesionales al día con las tecnologías y estrategias más recientes.

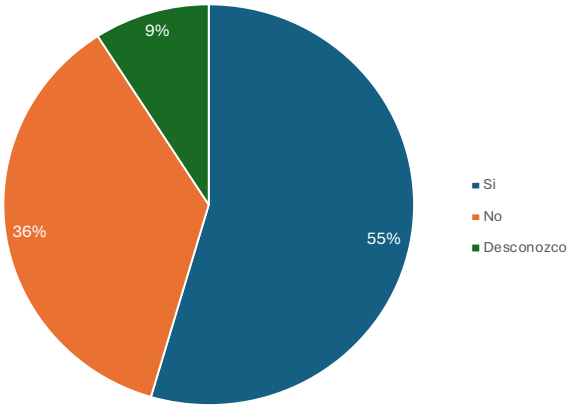
**Gráfico 2 Oferta de programas de formación en ciberseguridad en instituciones educativas**




**Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2023.**

Respecto a la disponibilidad de presupuesto exclusivo a actividades de investigación y desarrollo en ciberseguridad, los datos registran que aproximadamente de la mitad de las instituciones académicas participantes, un 54,5% de esta muestra, cuenta con un presupuesto destinado a la investigación y desarrollo en ciberseguridad, sin embargo, un 36,4% no dispone a recursos monetarios para iniciativas y proyectos de esta índole, mientras que un 9,1% desconoce del tema. Si bien, se identifica que la asignación de recursos para la investigación y el desarrollo (I+D) en ciberseguridad constituye un desafío notable, a pesar de la ausencia de presupuestos, más de la mitad de los participante sí ha llevado a cabo investigaciones de esta índole, lo que indica un esfuerzo notable por avanzar en el campo a pesar de las limitaciones financieras.

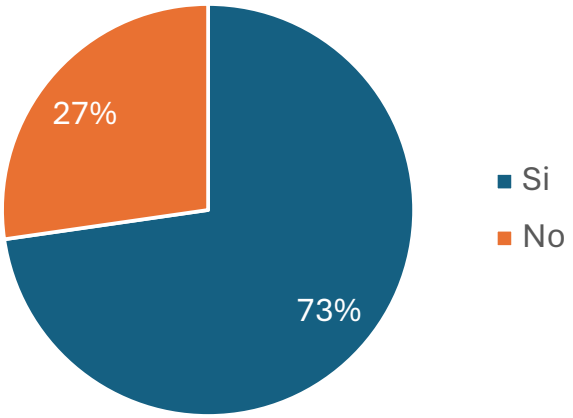
**Gráfico 3 Disponibilidad de presupuestos dedicados a actividades de I+D en ciberseguridad**




**Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2023.**

Un poco en línea con lo anterior, de las instituciones académicas encuestadas, un 54,5% detalla que efectivamente sí han llevado a cabo investigaciones en algún área relacionada a la ciberseguridad durante el 2023, mientras que un 45,5% indica que no ha efectuado investigaciones en este ámbito. No obstante, pese a la ausencia de estudios investigativos, los datos registran que una gran mayoría de instituciones académicas (72,7%) si cuentan con planes futuros para realizar proyectos de investigación y desarrollo en ciberseguridad, mientras que un 27,3% indica que no cuenta con planes futuros sobre este aspecto, por tanto, se evidencia una tendencia optimista, lo que sugiere un reconocimiento creciente de la importancia estratégica de la ciberseguridad y un compromiso para fortalecer este ámbito a largo plazo.

**Gráfico 4 Planes futuros de investigación y desarrollo en ciberseguridad**




**Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2023.**

En lo que concierne a percepción en cuanto a la relevancia de la investigación y desarrollo en ciberseguridad en institución académicas, un 54,5% lo categoriza como muy importante, un 27,3% lo considera simplemente importante, mientras que un porcentaje menor del 18,2% lo considera neutral en términos de relevancia, estos datos reflejan que en efecto existe una percepción positiva y relevante en torno a la I+D en ciberseguridad e inclusive implica compromiso institucional para abordar y mitigar los riesgos asociados a la seguridad de la información.

En última instancia, para finalizar esta sección de la encuesta, se invita a los encuestados a ofrecer comentarios adicionales o aportes relevantes en relación al estado actual de la investigación y desarrollo de la ciberseguridad en su institución. Si bien esta pregunta era de carácter opcional, algunas respuestas indican lo siguiente:

En principio, es fundamental para las instituciones educativas enfocarse en la investigación en el ámbito de la ciberseguridad, para incorporar estos conocimientos esenciales en sus programas formativos, contribuyendo así con profesionales que ayuden al fortalecimiento de la seguridad de la información en las organizaciones donde lleguen a colaborar. Aunado a esto, detallan que resulta vital avanzar en la recolección y análisis de datos que permitan mejorar las medidas de protección.

Por otra parte, indican que actualmente, las actividades de Investigación y Desarrollo (I+D) de las instituciones se centran en los proyectos de fin de carrera de los programas de Maestría, lo que subraya la importancia de expandir sus esfuerzos de investigación para abarcar una gama más amplia de temas y disciplinas.

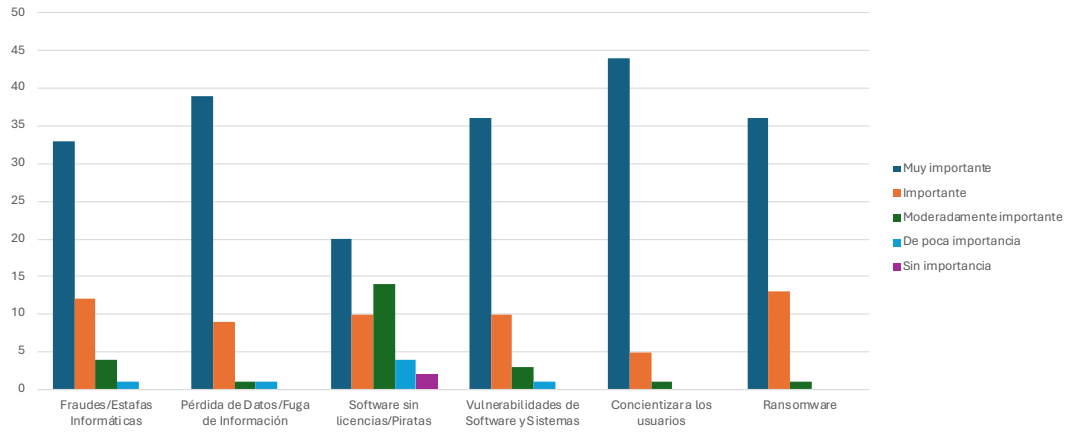
### 3.2.2. Situación Jurídica de la Ciberseguridad Nacional

#### 3.2.2.1. Seguridad Cibernética

Respecto a las mayores preocupaciones en materia de seguridad cibernética, los resultados reportan que una de las principales inquietudes gira en torno a la concientización de usuarios, pues un 88% considera muy importante este factor, particularmente por la relevancia en cuanto a la prevención de amenazas cibernéticas e inclusive por la ausencia de una cultura cibernética sólida; en segundo lugar se posiciona la pérdida de datos/ fuga de información con un 78%, en el sentido que representa una amenaza significativa para las empresas, pues dicha información puede contener datos sensibles y confidenciales, lo que pudiese impactar negativamente a las organizaciones.

En el caso de vulnerabilidades de software y sistemas, así como presencia de ransomware, 36 participantes indicaron que representan una de sus mayores preocupaciones, ocupando así el tercer lugar, en esencia debido a que este tipo de amenazas representan riesgos sustanciales en términos de confidencialidad e integridad. Por su parte, si bien un 66% de los encuestados encuentra los fraudes/estafas informáticas una de sus más importantes amenazas, este dato es ligeramente menos significativo en comparación con los demás factores. No obstante, los datos muestran que la presencia de software sin licencias/piratas no representa un factor tan importante, pues menos de la mitad de encuestados lo consideran de alta relevancia, específicamente un 40%, e inclusive un 4% insinúa que ni siquiera es objeto de relevancia en cuanto a preocupaciones cibernéticas.

**Gráfico 5 Preocupaciones en seguridad cibernética**

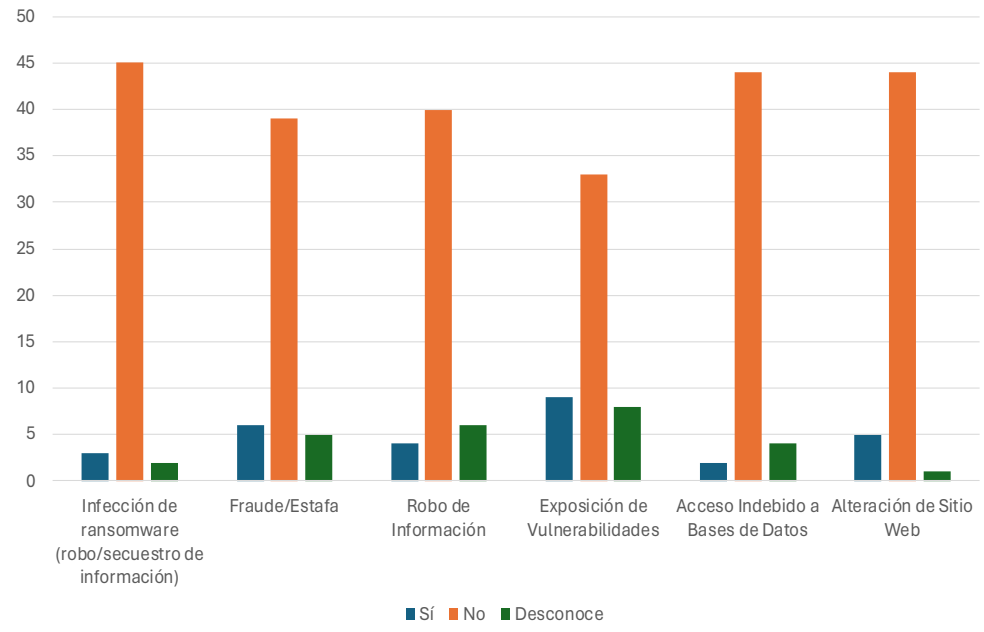



**Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2023.**

Si bien la encuesta evidencia que las organizaciones, indiferentemente de su pertenencia al sector público o privado, presentan inquietudes en torno a seguridad cibernética, la realidad es que los datos indican que al menos en el año 2023 gran parte de los encuestados no han experimentado o desconocen si han sufrido ataques de esta índole; cerca de un 90% señala que no han presentado ataques relacionados a infecciones de ransomware (robo/secuestro de información), accesos indebidos a bases de datos, así como alteraciones de sitio web, no obstante, este dato no implica necesariamente que esté exenta de riesgos o amenazas cibernéticas.

En el caso de fraudes/estafas y robo de información si bien un 78% y 80% respectivamente, no han sufrido ataques, este dato señala que la mayoría de los ciberataques giran en torno a estos incidentes, no obstante, se puede observar que la mayor cantidad de ataques informáticos a los que se vieron expuestos los participantes se relacionan con exposición de vulnerabilidades, seguido de fraudes/estafas y alteraciones de sitio web. Sin embargo, a pesar de experimentar ataques cibernéticos la encuesta registra que un 62% de las empresas no proceden a denunciar el ataque ante el Sistema Judicial, mientras que un 30% reconoce que desconoce si se continúa con este procedimiento, por tanto, únicamente un 8% realiza la denuncia frente a las autoridades pertinentes; ante esta situación se dificulta aún más la evaluación de incidentes e inclusive limita la capacidad de respuesta de las autoridades ante este tipo de delitos, y por ende el reconocimiento de la necesidad de estrategias para combatir los diferentes tipos de ciberataques.

**Gráfico 6 Ataques Cibernéticos**

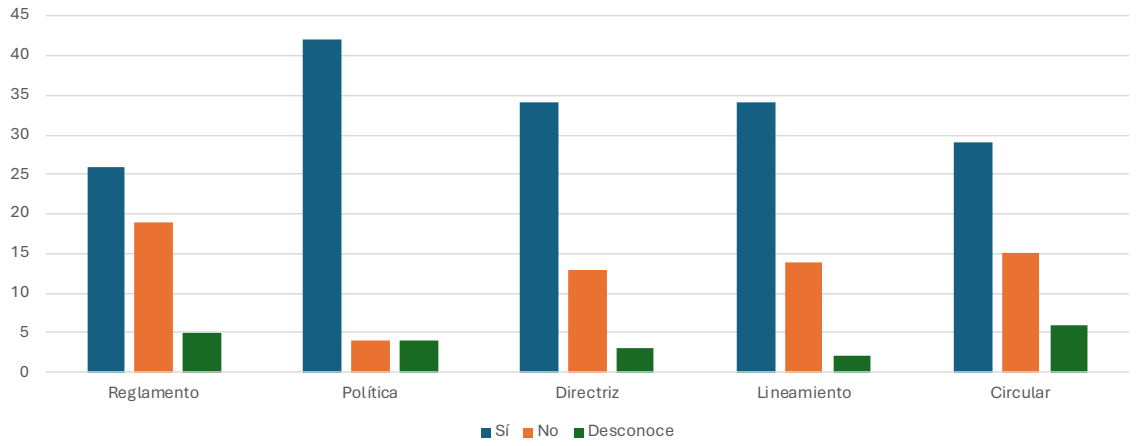



**Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2023.**

### 3.2.2.2. Estado de la Ciberseguridad

Con el objetivo de contextualizar el estado actual de las instituciones en materia de ciberseguridad es prudente determinar si las organizaciones disponen de protocolo de actuación ante un incidente en sus sistemas de información, por tanto, mediante la encuesta registra que un 70% de los participantes confirma que cuentan con procedimientos operativos de actuación ante incidencias informáticas, no obstante, un 26% indica que actualmente no disponen de protocolos de esta índole, mientras que únicamente un 4% desconoce del tema dentro de su organización.

**Gráfico 7 Establecimiento de normativas internas en materia de tecnologías**

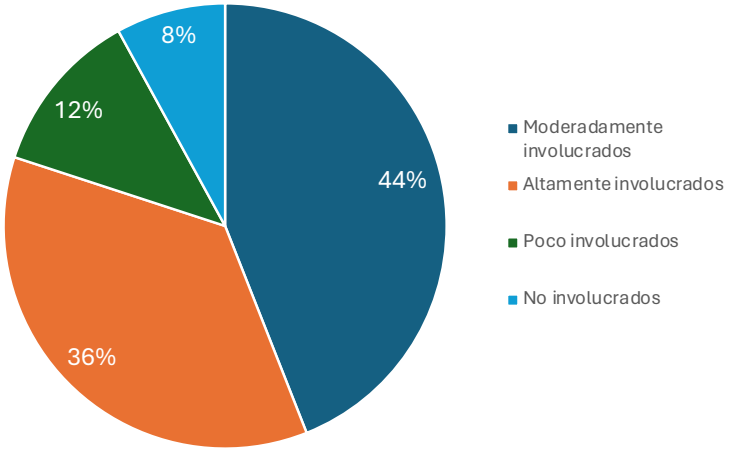



**Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2023.**

Un poco en línea con lo anterior, se evidencia que en materia de reglamentos, políticas, circulares o directrices, en su mayoría las organizaciones implementan políticas, específicamente un 84% de los participantes indican que emplean este tipo de normas sobre el uso de los equipos de tecnologías de la información, seguido de directrices y lineamientos, ambos con un 68%, asimismo, se registra que las normas menos utilizadas versan sobre circulares (58%) y reglamentos (52%).

Asimismo, en cuanto al nivel de involucramiento de la alta dirección en la decisiones y políticas relacionadas directamente a la ciberseguridad, los datos recopilados sugieren que 44% de las organizaciones encuestadas, la alta dirección se encuentra moderadamente involucrado, mientras que un 36% indica que un mayor nivel involucramiento, no obstante, una cifra significativa de un 12% implica que la dirección ejecutiva interfiere poco en decisiones en términos de ciberseguridad, y solamente un 8% indica que su involucramiento es inexistente o poco significativo.

**Gráfico 8 Involucramiento de la alta dirección en decisiones y políticas de ciberseguridad**



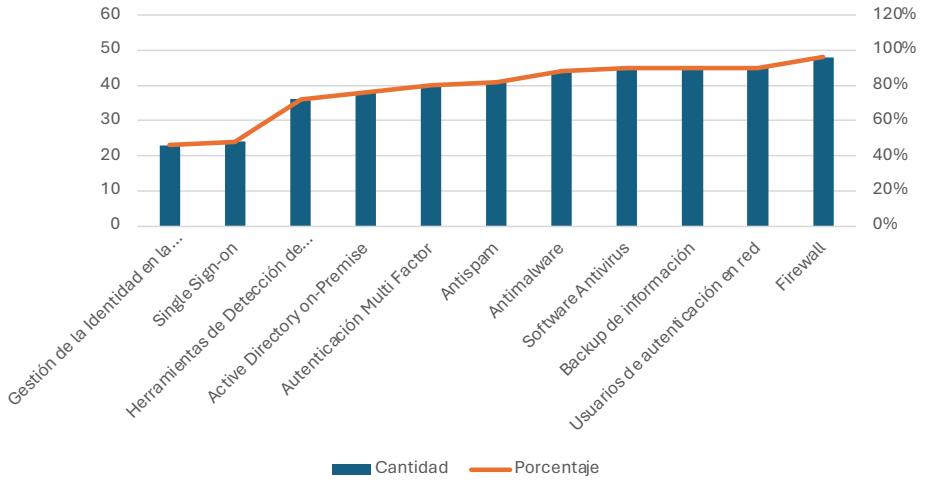

**Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2023.**

De igual modo, en relación a la comunicación de políticas de ciberseguridad, así como de prácticas al público interno de la organización, los resultados registran que este tipo de información generalmente es divulgada por medio de correos electrónicos y/o boletines (90%), asimismo, es relevante acotar que seguido de este medio, durante las reuniones y capacitaciones (52%) también se comparte información de esta índole, por último, un 38% de los participantes indicó que se realiza mediante portales internos.

A fin de garantizar la protección informática de sus sistemas, y como resultado de la preocupación ante amenazas cibernéticas, es relevante consultar sobre la existencia de revisiones periódicas del estado de la seguridad de los sistemas de información en las instituciones, pregunta a la cual el 80% de los encuestados señalaron que efectivamente realizan revisiones con regularidad, un 12% indican que no se efectúan dichas evaluaciones.

De acuerdo a los datos recopilados, se evidencia que entre los principales controles de seguridad cibernética, la mayoría de las organizaciones disponen de sistemas firewall (96%), software antivirus (92%), backup de información (90%), usuarios de autenticación en red (90%), antimalware (88%), antispam (84%) y programas de autenticación multi factor (80%).

**Gráfico 9 Controles de Seguridad Cibernética**



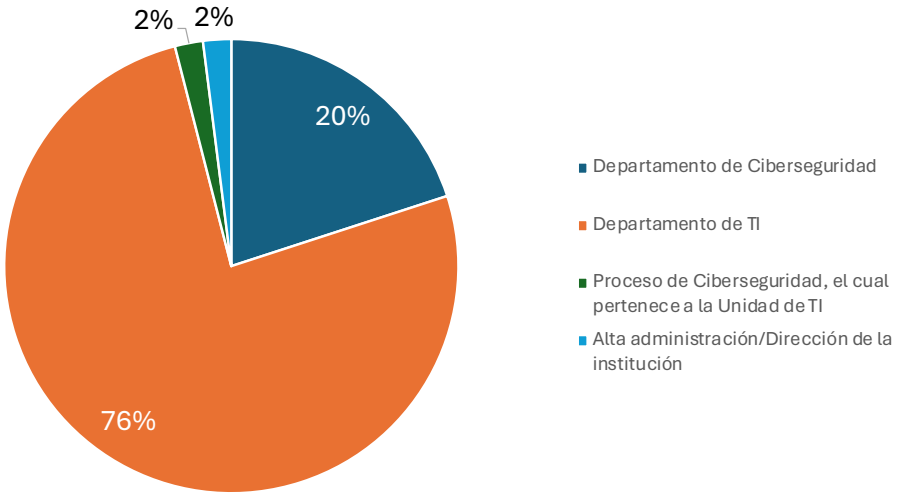

**Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2023.**

### 3.2.2.3. Prevención de Incidentes

En el contexto de la seguridad cibernética, especialmente en la prevención de incidentes, resulta fundamental determinar en cuál departamento recae este tipo de decisiones, en particular, los resultados de la encuesta sugieren que un 76% de las organizaciones asignan dichas responsabilidades al departamento de TI, un aspecto relevante corresponde a que 20% de los participantes señalan la existencia de un departamento de ciberseguridad, el cual se encarga de aspectos relacionados a esta materia.

De igual modo, en relación a la comunicación de políticas de ciberseguridad, así como de prácticas al público interno de la organización, los resultados registran que este tipo de información generalmente es divulgada por medio de correos electrónicos y/o boletines (90%), asimismo, es relevante acotar que seguido de este medio, durante las reuniones y capacitaciones (52%) también se comparte información de esta índole, por último, un 38% de los participantes indicó que se realiza mediante portales internos.

**Gráfico 10 Departamentos responsables de la prevención incidente cibernéticos**

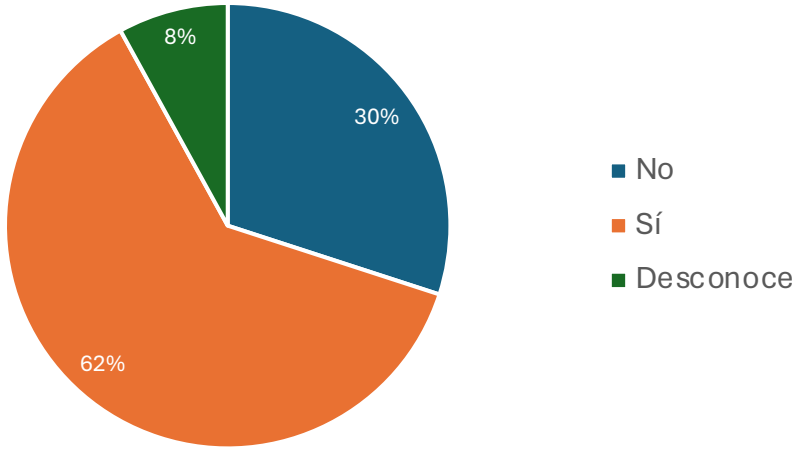



**Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2023.**

Siendo así, es prudente la identificación de mecanismos de prevención de incidentes en instituciones públicas y/o privadas, pues constituye un factor relevante en cuanto a protección de activos e información, así como para salvaguardar la integridad y confianza de las organizaciones. De manera que, se evidencia que un 62% de las instituciones encuestadas efectivamente implementan algún tipo de evaluación ante riesgos cibernéticos, 30% no ejecuta ningún mecanismo de control, y únicamente un 8% desconoce de la existencia de este tipo de procedimientos.

Siendo así, es prudente la identificación de mecanismos de prevención de incidentes en instituciones públicas y/o privadas, pues constituye un factor relevante en cuanto a protección de activos e información, así como para salvaguardar la integridad y confianza de las organizaciones. De manera que, se evidencia que un 62% de las instituciones encuestadas efectivamente implementan algún tipo de evaluación ante riesgos cibernéticos, 30% no ejecuta ningún mecanismo de control, y únicamente un 8% desconoce de la existencia de este tipo de procedimientos.

**Gráfico 11 Implementación de mecanismo de evaluación de riesgo cibernético**

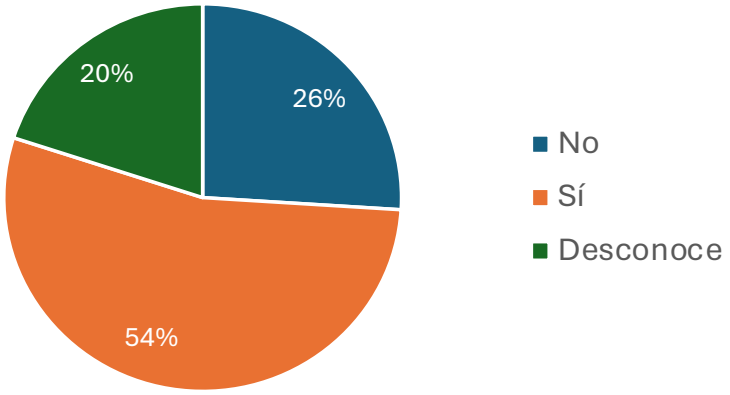



**Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2023.**

En línea con lo anterior, los resultados obtenidos sugieren que un 76% de las organizaciones restringen el acceso a la red desde dispositivos personales no gestionados como medida de prevención ante ciberamenazas, mientras que un 24% no restringe el acceso de este tipo de dispositivos dentro de la institución. No obstante, en cuanto a la regularización del uso de plataformas digitales tales como Facebook, Instagram o Twitter (actualmente X), etc., más de la mitad de los encuestados (56%) señalan la inexistencia de reglamentos, protocolos, políticas, directrices o circulares dedicados al control de redes sociales, por lo que únicamente el 44% emplea normativas en torno a este tema.

Dentro del marco jurídico actual, la protección de datos del cliente constituye un pilar fundamental en términos de derechos humanos, razón por la cual debe ser priorizados en políticas, estrategias y planes de acción, mediante la encuesta se determina que un 54% de los participantes cuenta con medidas en materia técnica para cumplir la ley de protección de datos del cliente, mientras que 26% no dispone de medidas de esta índole, y un 20% desconoce de la aplicación de estas medidas, resultados un poco alarmantes actualmente, especialmente en el auge y consolidación de la era digital.

**Gráfico 12 Implementación de medidas para el cumplimiento de la ley de protección de datos del cliente**

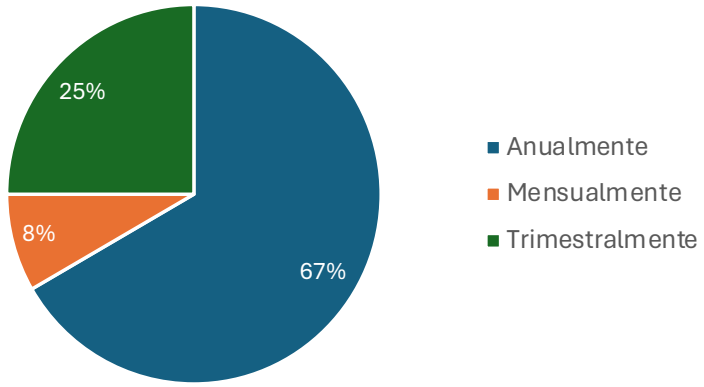



**Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2023.**

En lo que concierne a la mayor amenaza que perciben las instituciones, se evidencia que un 72% de las organizaciones consideran que tanto internamente como externamente se encuentran vulnerables cibernéticamente, por su parte, con una porcentaje menos significativo se encuentran aquellas que únicamente perciben que dichas amenazas son únicamente internas (12%) o externas (12%). Sin embargo, pese a estos datos, es prudente señalar que la encuesta registra que un 48% de las empresas realiza pruebas de phishing o simulacros de seguridad para evaluar la preparación de los empleados ante incidentes informáticos, por ende, un 42% no procede a realizar este tipo de mecanismos de seguridad, lo cual representa un porcentaje preocupante, esto en el sentido que representa una brecha significativa en medidas de seguridad al aumentar su 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 que la frecuencia de este tipo de simulacros en su mayoría (66,7%) se realiza anualmente, 25% lo realiza a cabo trimestralmente, mientras que un porcentaje muy pequeño (8,3%) ejecuta estos procedimientos mensualmente.

**Gráfico 13 Frecuencia de simulaciones**



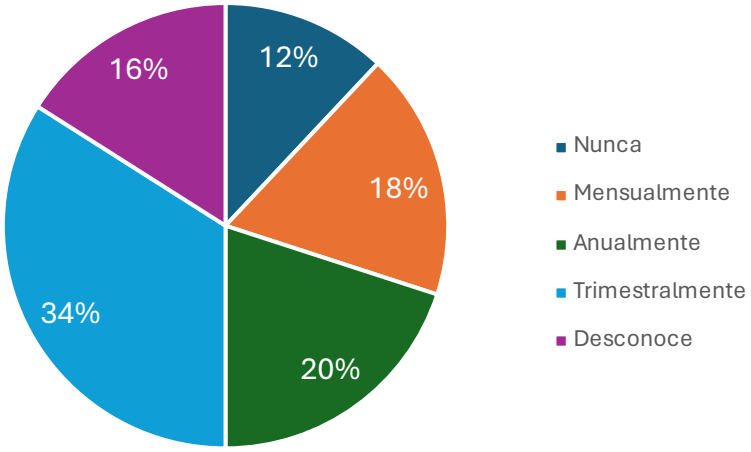

**Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2023.**

### 3.2.2.4. Programas de capacitación y/o formación

El panorama actual plantea oportunidades y desafíos para el ámbito de la ciberseguridad, motivo por el cual es relevante determinar si las organizaciones cuenta con iniciativas en materia de investigación y desarrollo en ciberseguridad I+D+i , pregunta a la cual un 60% de los participantes detallan que no existen iniciativas o acciones en temas de seguridad, por lo que únicamente un 40% de los encuestados si realiza programas de este tipo. No obstante, se registra que el 72% de los encuestados participa u organiza en conferencias y/o talleres sobre ciberseguridad, particularmente, 34% de las organizaciones asiste trimestralmente, 20% anualmente, 18% mensualmente, mientras que el 28% detalla que desconoce del dato (16%) o afirma que no se realizan este tipo de eventos (12%).

En lo que concierne a la mayor amenaza que perciben las instituciones, se evidencia que un 72% de las organizaciones consideran que tanto internamente como externamente se encuentran vulnerables cibernéticamente, por su parte, con una porcentaje menos significativo se encuentran aquellas que únicamente perciben que dichas amenazas son únicamente internas (12%) o externas (12%). Sin embargo, pese a estos datos, es prudente señalar que la encuesta registra que un 48% de las empresas realiza pruebas de phishing o simulacros de seguridad para evaluar la preparación de los empleados ante incidentes informáticos, por ende, un 42% no procede a realizar este tipo de mecanismos de seguridad, lo cual representa un porcentaje preocupante, esto en el sentido que representa una brecha significativa en medidas de seguridad al aumentar su exposición ante ataques informáticos.

**Gráfico 14 Participación/organización de conferencias o talleres sobre ciberseguridad**

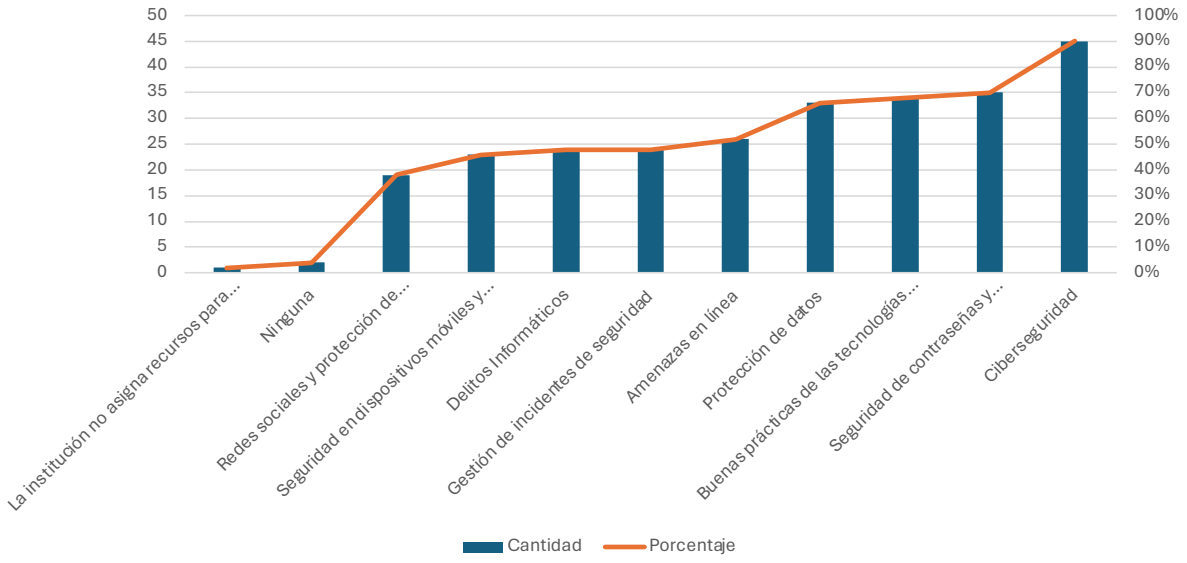



**Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2023.**

Respecto a programas de formación, entre las temáticas más relevantes, es válido señalar que un 90% de las organizaciones sugieren que el personal ha recibido capacitaciones sobre ciberseguridad, un 70% sobre seguridad de contraseñas y autenticación de doble factor, así como buenas prácticas de las tecnologías de información (TI), 66% sobre protección de datos, y un 54% sobre amenazas en línea.

Respecto a programas de formación, entre las temáticas más relevantes, es válido señalar que un 90% de las organizaciones sugieren que el personal ha recibido capacitaciones sobre ciberseguridad, un 70% sobre seguridad de contraseñas y autenticación de doble factor, así como buenas prácticas de las tecnologías de información (TI), 66% sobre protección de datos, y un 54% sobre amenazas en línea.

**Gráfico 15 Temáticas de formación y/o capacitación**




**Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2023.**

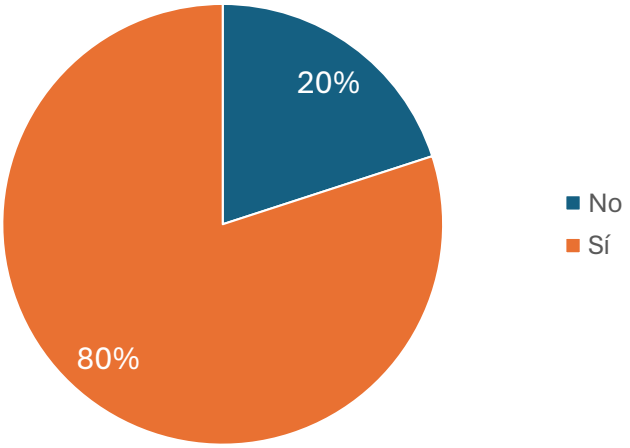
### 3.2.2.5. Procedimiento Legal

Con 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, el 80% de los encuestados dice conocer la normativa relacionada, y al mismo tiempo el 92% piensa que no es suficiente con respecto a los incidentes informáticos, siendo contradictorio con respecto al porcentaje que indica que si la conoce.

### 3.2.2.5. Procedimiento Legal

Con 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, el 80% de los encuestados dice conocer la normativa relacionada, y al mismo tiempo el 92% piensa que no es suficiente con respecto a los incidentes informáticos, siendo contradictorio con respecto al porcentaje que indica que si la conoce.

**Gráfico 16 Conocimiento de la ley de delitos informáticos**



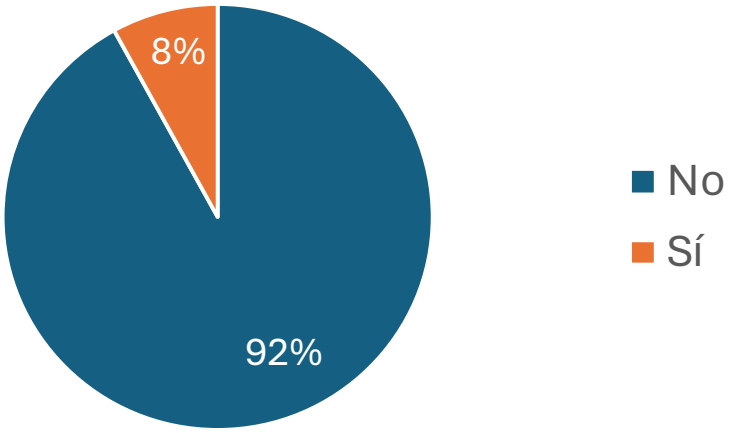

**Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2023.**

Si bien el desarrollo cambiante en materia de tecnología hace que los temas legales deban tener una actualización constante, lo cual sería lo idea, estos datos podrían reflejar que falta aún formación en los diferentes sectores para dar a conocer los delitos informáticos con los que contamos y cómo aplica, esto para poder reflejar si realmente consideran que no cubre los actuales escenarios, siendo que a nivel internacional la normativa costarricense en materia de tecnología, y específicamente en delitos informáticos, es en lo que mejor hemos salido calificados por organismos internacionales como los estudios realizados por la Organización de Estados Americanos, y estos vacíos del conocimiento legal y del procedimiento penal lo vemos reflejado en las respuestas dadas con respecto al motivo de que consideren la normativa insuficiente:

- No he leído la ley
- Es bastante superficial
- La Ley debe actualizarse ya que cada día hay nuevos esquemas y mecanismos empleados por los cibercriminales.
- No cuenta con la especificidad apropiada
- En lo personal se debe incluir normativa que proteja al usuario cuando sufre un delito que no fue ocasionado por el usuario, si no por la falta de medidas de seguridad de las entidades bancarias y se debe hablar de sanciones de estas entidades.
- Aún hay algunos días nublados del día en nuestra legislación.
- No conozco la ley, es una tarea por realizar
- Si los cubriera estaríamos protegidos con las estafas en los bancos
- No la conozco
- No la he estudiado
- Porque no la he estudiado
- A pesar de la existencia de vasta de información en el tema de delitos informáticos, carece de un instrumento de aplicación y ejecución.
- Está desactualizada
- Son leyes retrogradas que no protegen la información de las empresas y las organizaciones ni se adecuan a los tiempos y los avances tecnológicos
- En realidad, no estamos seguro por falta de conocimiento del tema
- Si bien se la han realizado algunas actualizaciones, aún está lejos de estar al nivel de normativas de países y regiones más desarrollados

Muchos de los comentarios van enfocados a la no lectura de la normativa o falta de conocimiento en materia de derecho penal y procesal penal que pueden estar generando una confusión con respecto a los alcances en materia penal, sus etapas y los procedimientos que se realizan.

**Gráfico 17 Percepción sobre si la cobertura de la ley de incidentes informáticos en Costa Rica es adecuada**




**Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2023.**

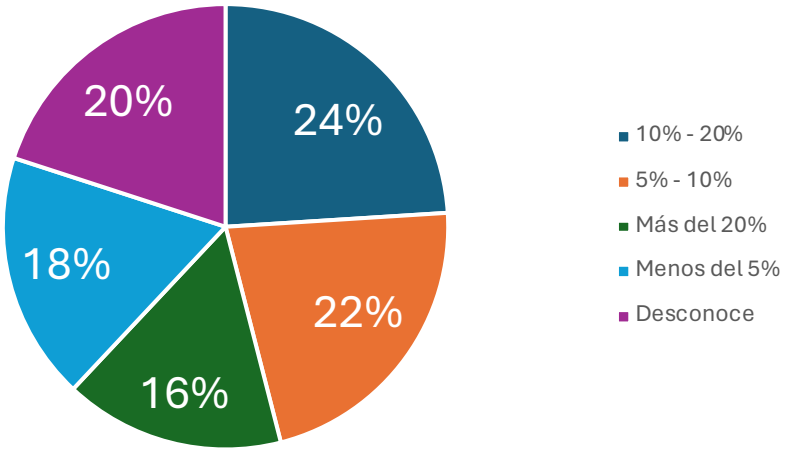
### 3.2.2.6. Recursos y Presupuesto

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 de su organización, se asigna una sección específica, ya que la inversión en ciberseguridad se puede traducir como medidas preventivas, sistemas de detección e inclusive capacidad de respuesta, así como programas de formación y capacitación. Siendo así, los resultados determinan que en relación con el porcentaje del presupuesto de TI destinado a ciberseguridad, 24% asigna un porcentaje entre del 10%-20%, 22% de los participantes 5%-10%, 20% desconoce del monto, 18% estima un porcentaje menor al 5% y finalmente un 16% asigna fondos mayores al 20%.  A pesar de este contexto, el 70% de los encuestados considera que este presupuesto no es adecuado a las necesidades actuales en materia de ciberseguridad.

### 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 de su organización, se asigna una sección específica, ya que la inversión en ciberseguridad se puede traducir como medidas preventivas, sistemas de detección e inclusive capacidad de respuesta, así como programas de formación y capacitación. Siendo así, los resultados determinan que en relación con el porcentaje del presupuesto de TI destinado a ciberseguridad, 24% asigna un porcentaje entre del 10%-20%, 22% de los participantes 5%-10%, 20% desconoce del monto, 18% estima un porcentaje menor al 5% y finalmente un 16% asigna fondos mayores al 20%.  A pesar de este contexto, el 70% de los encuestados considera que este presupuesto no es adecuado a las necesidades actuales en materia de ciberseguridad.

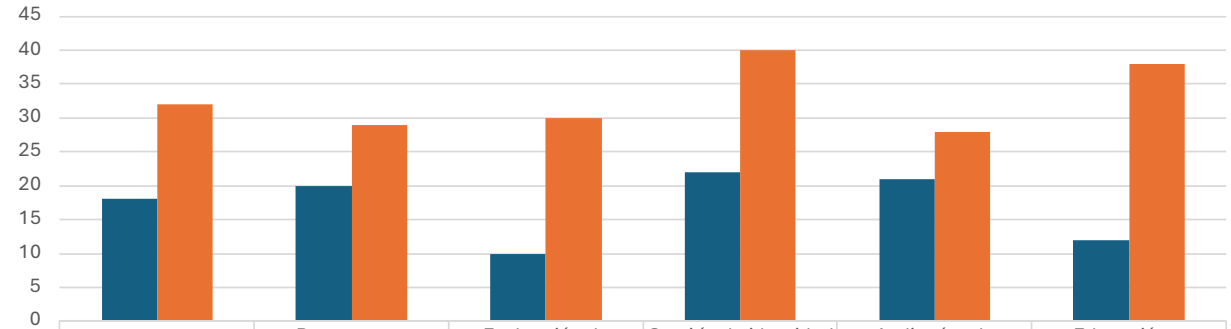
**Gráfico 18 Asignación porcentual del presupuesto de TI destinado a ciberseguridad**




**Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2023.**

En relación con lo anterior, es importante reconocer si las organizaciones participantes subcontratan servicios relacionados con ciberseguridad, en principio, los datos recopilados demuestran que más de la mitad de encuestados no subcontratan o adquieren servicios de esta índole. No obstante, entre los servicios más contratados se encuentra el servicio de auditorías de seguridad (44%), respuesta a incidentes (42%), evaluación de vulnerabilidades (40%) y monitoreo (36%), por su parte, los menos adquiridos giran en torno a educación o concientización (12%) y el servicio de gestión de identidad y acceso con únicamente un 20%.

**Gráfico 19 Subcontratación de Servicios**



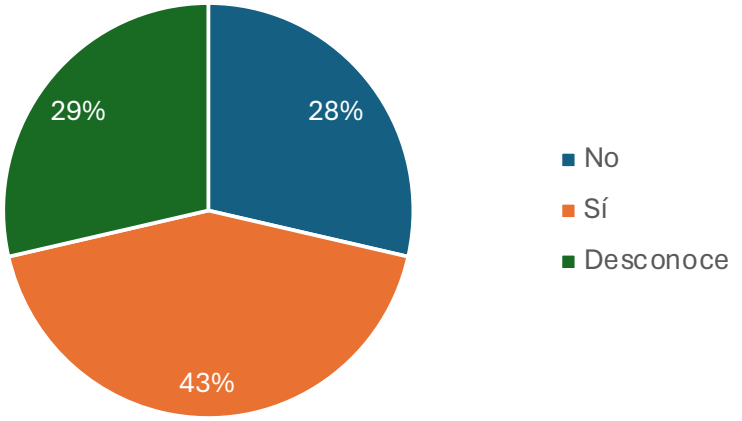

| | Monitoreo | Respuesta a incidentes | Evaluación de vulnerabilidades | Gestión de identidad y acceso | Auditorías de seguridad | Educación o concientización |
|---|---|---|---|---|---|---|
| Sí | 18 | 20 | 10 | 22 | 21 | 12 |
| No | 32 | 29 | 30 | 40 | 28 | 38 |

**Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2023.**

### 3.2.2.7. Alcance Operativo

En virtud de la relevancia del contexto cibernético, es prudente identificar si aquellas organizaciones que desarrollen actividades en mercados extranjeros realizan evaluaciones particulares para cada uno de los mercados donde opera, pues implica análisis de riesgos, cumplimiento jurídico e incluso adaptación de estrategias. En primera instancia, únicamente un 28% de las organizaciones encuestadas tienen un alcance operativo en mercados internacionales, específicamente 92,9% opera en América Central, 64,3% en América del Sur, 42,9% en América del Norte, 28,6% en Europa, un porcentaje de 14,3% en África, Asia y Oceanía, respectivamente, y un porcentaje inferior (7,1%) en Medio Oriente.

**Gráfico 20 Evaluación de riesgos en mercados internacionales**




**Fuente: LabCIBE-UNA, Encuesta Estado de la Ciberseguridad: Situación Jurídica, Investigación y Desarrollo, 2023.**

De acuerdo con los datos recopilados, en el gráfico 20 se puede evidenciar el 42,9% de las organizaciones que operan en el extranjero llevan a cabo evaluaciones de riesgo individuales en cada uno de los mercados en donde desarrolla actividades económicas, mientras que un 28,6% sugiere que no se realiza, otro 28,6% alega que desconoce si se procede con este tipo de medida preventiva. Sin embargo, en cuanto a protección de comunicaciones internas y externas mediante alguna red privada virtual (VPN) o tecnologías de seguridad similares, el 92,9% asegura que efectivamente se implementan dichos mecanismos en sus empresas.

# CONCLUSIONES

WWW.UNA.AC.CR

MIEMBRO ACTIVO · Cybersec Cluster · MIEMBRO ACTIVO

LABORATORIO DE I+D+i
LABCIBE
EN CIBERSEGURIDAD

VICERRECTORÍA DE INVESTIGACIÓN
UNIVERSIDAD NACIONAL

UNA
UNIVERSIDAD NACIONAL
COSTA RICA
SEDE REGIONAL CHOROTEGA

# Conclusiones

En Costa Rica, un 90,9% de las instituciones académicas imparten formación en ciberseguridad y un 81,8% establece colaboraciones con empresas a través de convenios, demostrando la existencia de un fuerte compromiso en fomentar este tipo de educación especializada. Esta interacción entre el sector académico y las empresas subraya la importancia de crear sinergias para la formación efectiva en ciberseguridad, esencial para que los futuros profesionales puedan aplicar sus conocimientos en escenarios reales y resolver problemas de manera efectiva.

La proyección a futuro indica que el 72,7% de las instituciones académicas planea iniciar proyectos de I+D en ciberseguridad, reflejando así una conciencia creciente sobre el valor estratégico de la ciberseguridad y una determinación para reforzar este campo de manera sostenida. Sin embargo, sobre la asignación de recursos para I+D en ciberseguridad existe un desafío considerable, un 54,5% de las instituciones indican la falta de presupuestos dedicados a este fin, a pesar de estas limitaciones financieras, este porcentaje de instituciones ha logrado ejecutar con éxito la investigación y desarrollo en el área.

De manera que, surge la afirmación de que las actividades de I+D en ciberseguridad se limitan principalmente a los proyectos de fin de carrera de los programas de postgrado en las instituciones académicas, aunque este instrumento no ha sacado datos concluyentes para respaldar esta afirmación, razón por la cual esta cuestión se tomará en cuenta para la próxima versión del instrumento. No obstante, sí cabe resaltar la importancia de ampliar las iniciativas de I+D de parte de las instituciones académicas, y llevarlas más allá de los trabajos de graduación, por ejemplo a través de la extensión universitaria.

El escenario actual ofrece la oportunidad de crear un centro especializado en innovación, investigación y desarrollo para abordar los desafíos que tienen los diversos sectores de la industria nacional, incluidas las empresas, las comunidades, infraestructuras críticas y el ámbito académico, entre otras. Este centro tendría como meta coordinar esfuerzos de I+D en ciberseguridad con diversos actores. Obteniendo como beneficio el formar profesionales capacitados con experiencia en ciberseguridad. Así como desarrollar soluciones relevantes a los retos nacionales, investigar nuevas tecnologías, y en general fomentar la innovación en ciberseguridad en Costa Rica, contribuyendo al avance y seguridad del país.

Desde la perspectiva jurídica, es evidente que Costa Rica actualmente enfrenta el reto de fortalecer su gestión en ciberseguridad, área en la que aún no se ha consolidado una dirección, control y manejo efectivos, por lo que es crucial que el Gobierno, desde el MICITT, asuma un papel protagónico en este campo. De manera que, es esencial el poder desarrollar la Estrategia Nacional de Ciberseguridad, instrumento el cual guiará a los encargados de la ciberseguridad en Costa Rica, promoviendo una coordinación efectiva entre todas las entidades involucradas, para superar los actuales retos en ciberseguridad del país.

Aunado a esto, es importante recordar que la tecnología en sí no es el problema; por el contrario, es parte de la solución, en el sentido que, la protección y uso seguro de las tecnologías no son responsabilidades exclusivas del Gobierno, sino que también recaen en instituciones autónomas, el sector privado y el empresarial; por tanto, todos son corresponsables, no obstante, es el Gobierno es quien debe liderar y dirigir los esfuerzos en ciberseguridad, recordando que es imperativo considerar el ciberespacio como un elemento central en la gestión de riesgos de la seguridad nacional. Esto implica asignar los recursos necesarios a las instituciones para combatir la ciberdelincuencia, lo que debe complementarse con convenios internacionales y legislaciones que siempre se pueda revisar y actualizar.

Finalmente, es necesario que las normativas relacionadas con la tecnología sean revisadas desde una perspectiva técnica, para asegurar que la legislación sea aplicable en el ámbito tecnológico, recordando que esto requiere un equilibrio entre las áreas jurídica e informática, para lograr normativas que sean tanto eficientes como efectivas.

Resultado del análisis y resultados en materia de ciberseguridad y derecho, se identifican varias áreas clave de preocupación y acción. En primer lugar, se destaca la importancia de la concientización de los usuarios y la protección de datos, resaltando la necesidad urgente de fortalecer la cultura cibernética y desarrollar medidas más efectivas para salvaguardar información sensible y confidencial. Otro aspecto para considerar, es la incidencia de los ciberataques y la subsecuente respuesta a estos, pues a pesar de que muchos encuestados indican no haber experimentado ciberataques, se observa una preocupante baja tasa de denuncias en los casos que sí ocurren, esta situación limita significativamente la capacidad de las autoridades para responder y evaluar adecuadamente estos incidentes, lo que podría tener implicaciones en la seguridad nacional y en la confianza de las instituciones y el público, a pesar de que existan normativa para denunciar estos hechos, teniendo en cuenta que el caso del sector público es una obligación denunciar cualquier delito que ocurra.

En cuanto a la gestión y las políticas de ciberseguridad, se nota que un número considerable de organizaciones ha implementado protocolos para actuar ante incidentes cibernéticos. Estos protocolos, junto con políticas enfocadas en el uso seguro de las tecnologías de la información, son pasos importantes hacia la mitigación de riesgos cibernéticos, pero a su vez el papel de la alta dirección en estas políticas y decisiones varía considerablemente entre las organizaciones, esta variabilidad en el nivel de involucramiento puede influir en la eficacia con que se implementan y se ejecutan las estrategias de seguridad cibernética, siendo fundamental que se genere una participación activa y comprometida de los líderes para asegurar una defensa robusta contra las amenazas cibernéticas.

Por último, se reconoce una percepción general de que la legislación existente en torno a los delitos informáticos es insuficiente y requiere una actualización para abordar adecuadamente los desafíos emergentes en ciberdelincuencia, si bien se denota esta situación en la percepción de los encuestados, y que sea importante la necesidad de una revisión y adaptación continua de las leyes para mantenerse a la par con los avances tecnológicos y las tácticas cambiantes de los cibercriminales, si es necesario formar a la comunidad técnica, y a la ciudadanía en general, el conocer la existencia de delitos informáticos y cómo funciona el proceso penal, esto al ver el desconocimiento del mismo que existe entre la comunidad técnica.

De manera que, ante este escenario se recomienda:

Evaluación y Mejora de la Legislación y Regulación de la Ciberseguridad: Si bien nuestra normativa ha sido evaluada positivamente, es importante revisar y actualizar la legislación y regulaciones actuales para asegurar que estén alineadas con las tecnologías emergentes y las amenazas cibernéticas actuales. Esto puede incluir la creación de leyes más específicas en áreas como la protección de datos, la respuesta ante incidentes cibernéticos y sanciones para actividades delictivas en línea. Fortalecimiento de la Investigación y Desarrollo en Ciberseguridad: Incrementar la inversión en I+D en ciberseguridad, tanto a nivel gubernamental como privado.

Fomentar la colaboración entre universidades, empresas y entidades gubernamentales para impulsar la innovación y el desarrollo de soluciones avanzadas en ciberseguridad.

Creación de un Centro de Innovación, Investigación y Desarrollo en Ciberseguridad: Establecer un centro nacional de ciberseguridad que funcione como un hub para la investigación, la innovación y el desarrollo de soluciones de ciberseguridad. Este centro podría facilitar la colaboración entre diferentes sectores, servir como un recurso para la formación y capacitación avanzada, y ayudar a traducir la investigación académica en aplicaciones prácticas.

# BIBLIOGRAFÍA


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.*

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

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

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 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

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 1º 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

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

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/

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

# ESTADO DE LA CIBERSEGURIDAD EN COSTA RICA

# 2023

WWW.UNA.AC.CR

MIEMBRO ACTIVO · Cybersec Cluster · MIEMBRO ACTIVO

LABORATORIO DE I+D+i LABCIBE EN CIBERSEGURIDAD

VICERRECTORÍA DE INVESTIGACIÓN UNIVERSIDAD NACIONAL

UNA UNIVERSIDAD NACIONAL COSTA RICA SEDE REGIONAL CHOROTEGA