CIBERSEGURIDAD
Y
GOBERNANZA
EN LA ERA DIGITAL



La privacidad digital constituye un derecho; protegerla y preservar la seguridad es un deber compartido.

Carmen Carolina Ortega Hernández

UNIVERSIDAD AUTONOMA DE CHIAPAS
UNACH
POR LA CONCIENCIA DE LA NECESIDAD DE SERVIR

CIBERSEGURIDAD Y GOBERNANZA EN LA ERA DIGITAL

CIBERSEGURIDAD Y GOBERNANZA EN LA ERA DIGITAL

Carmen Carolina Ortega Hernández

Universidad Autónoma de Chiapas

2026

La modalidad mixta en la educación superior en México

ISBN DIGITAL: 978-607-561-435-9

D.R. © 2026. Universidad Autónoma de Chiapas
Boulevard Belisario Domínguez Km. 1081 sin número, Terán,
C.P. 29050, Tuxtla Gutiérrez, Chiapas, México

Coordinador editorial: Luis Adrián Maza Trujillo

Diseño editorial: María Beatriz Arévalo Dorry

Imagen de portada: Generada mediante inteligencia artificial con ChatGPT (OpenAI, 2026)

Cuidado Editorial: Dr. Samuel de Jesús Laparra Méndez

La Universidad Autónoma de Chiapas forma parte la Red Nacional de Editoriales Universitarias y Académicas de México, Altexto y de la Asociación de Editoriales Universitarias de América Latina y el Caribe, EULAC.

Las opiniones expresadas por los autores no necesariamente reflejan la postura del editor de la publicación o de la Universidad Autónoma de Chiapas; la información y análisis contenidos en esta publicación son estrictamente responsabilidad de los autores. Se autoriza la reproducción parcial o total de los textos aquí publicados, siempre y cuando se haga sin fines comerciales y se cite la fuente completa. Las imágenes de portada, la composición de interiores y el diseño de cubierta son propiedad de la Universidad Autónoma de Chiapas.

Hecho en México
Made in Mexico

Contenido

DEDICATORIA 11

ACERCA DE LA AUTORA 13

PRESENTACIÓN 15

PRÓLOGO 17

INTRODUCCIÓN GENERAL 19

OBJETIVO GENERAL 23

Capítulo 1.

Ciberseguridad Estratégica, Gobernanza y Gestión del Riesgo 25

Introducción. 25
Hacia una Ley Federal de Ciberseguridad. 26
Marco jurídico mexicano aplicable a las tecnologías
de la información, la transformación digital y la ciberseguridad. 30
Análisis comparativo del contenido de las iniciativas
de ley en materia de ciberseguridad. 37
Propuesta de integración de un catálogo de ciberdelitos
para una ley federal de ciberseguridad. 45
Gobernanza de las plataformas digitales:
la experiencia europea DMA y DSA 53
Gobernanza de la ciberseguridad y gestión del riesgo. 56
ISO/IEC 27001 como modelo de gobernanza. 63

Capítulo 2.

Seguridad Técnica e Infraestructura Digital 71

Introducción ... 71
Buenas prácticas con bases de datos ... 73
Vulnerabilidades en bases de datos ... 75
Técnicas de ataque y reconocimiento ... 80
Controles de protección para aplicaciones web ... 86
Buenas prácticas para plataformas digitales ... 90
Mensajería instantánea ... 90
Redes sociales ... 93
Correo electrónico ... 97
Dispositivos móviles y computadores ... 102
Aplicaciones ... 106
Navegación y entornos web ... 110
Medidas para la mitigación del Riesgo ... 114

Capítulo 3.

Cultura de Seguridad, Factor Humano y Protección de Datos 117

Introducción ... 117
Buenas prácticas con contraseñas ... 118
Código de acceso ... 120
Registro y almacenamiento de contraseñas ... 121
Tipos de acceso no autorizados ... 121
Casos de análisis para la cultura de ciberseguridad ... 127
Caso 1. ¿El derecho humano de acceso a internet autoriza el uso de una red WiFi privada sin consentimiento? ... 127
Caso 2. ¿Invertir en plataformas digitales garantiza la seguridad del patrimonio? ... 133
Caso 3. ¿Un manual de políticas de seguridad informática es realmente necesario? ... 139

Reflexiones 145

Glosario 147

Referencias 159

Anexos 167
Anexo 1. Matriz completa de las iniciativas
de Ley de Ciberseguridad en México. 169
Anexo 2. Matriz completa de las iniciativas
de reforma a la Ley de Seguridad Nacional de México. 180
Anexo 3. La organización y su contexto. 182
Anexo 4. Manual de Políticas de Seguridad Informática. 188

DEDICATORIA

Ciberseguridad y Gobernanza en la Era Digital nace con gratitud, ante todo a Dios por la oportunidad de vida que concede cada día; a las compañeras de cuna: Claudia, Irene y Nora; a los motores que inspiran a dar lo mejor: Carolina, Gilberto, Mayvelyn y Mía; a quienes dejaron un legado de servicio: Gloria y Pablo; y al compañero que camina a la par, alentando siempre a dar lo mejor.

Dra. Carmen Carolina Ortega Hernández

Acerca de la autora



Carmen Carolina Ortega Hernández es egresada de la Licenciatura en Informática del Instituto Tecnológico, de la Maestría en Ciencias de la Computación, de la Universidad Autónoma de Guadalajara, y del Doctorado en Administración de la Universidad del Sureste.

Es académica de la Universidad Autónoma de Chiapas, donde ha participado en los programas de Licenciatura en Sistemas Computacionales, Ingeniería en Desarrollo y Tecnologías de Software, Contaduría, Gestión de la Micro, Pequeña y Mediana Empresa y la Maestría en Administración. Ha colaborado en actividades de gestión académica como consejera técnica, presidenta de academia, coordinadora de programas de estudio, de acreditación y egresados. En el ámbito de la gestión universitaria ha ocupado distintos cargos, como directora en la Facultad de Negocios, y coordinadora en la Secretaría para la Inclusión Social y Diversidad Cultural, y en el Centro de Educación Continua y a Distancia, así como responsable del Programa Universitario de Inteligencia Artificial.

Su trayectoria como investigadora ha sido reconocida por la Secretaría de Ciencia, Humanidades, Tecnología e Innovación (SECIHTI) y el Instituto de Ciencia, Tecnología e Innovación de Chiapas (ICTICH), obteniendo la certificación Nacional Nivel I y

Estatal Nivel II. Está acreditada como Académica en Informática Administrativa por la Asociación Nacional de Facultades y Escuelas de Contaduría y Administración (ANFECA), y es integrante de la Asociación Nacional de Instituciones de Educación en Tecnologías de la Información (ANIEI). Asimismo, forma parte del padrón de evaluadores del Consejo Nacional de Acreditación en Informática y Computación (CONAIC), y también de SECIHTI e ICTICH.

Es autora del libro *Auditoría en Informática, asistida por tecnología con dictamen y sugerencias*, de artículos de revistas y capítulos de libros de prestigio nacional e internacional. Disfruta las oportunidades que le brinda la vida, fortaleciendo la difusión del conocimiento y la vinculación con la comunidad.

PRESENTACIÓN

Escribir representa la oportunidad de devolver a la sociedad parte de los conocimientos adquiridos durante la formación personal y profesional, con el propósito de compartir, de manera responsable, ética y solidaria, experiencias y reflexiones que contribuyan a fortalecer el conocimiento y a generar nuevas formas de comprender la realidad.

Toda obra aspira a trascender no por el número de sus páginas, sino por el valor de las ideas que comparte y por el impacto que éstas generan en quienes la leen. Con esa convicción, la presente publicación nace de la experiencia desarrollada en la docencia, la investigación, la gestión universitaria y la divulgación del conocimiento. Desde estas experiencias, se comparte una visión de la ciberseguridad que reconoce su carácter multidisciplinario y la necesidad de abordarla desde diferentes perspectivas.

La lectura busca crear un vínculo con el lector para reflexionar sobre los desafíos que plantea la sociedad digital frente al crecimiento de las amenazas que afectan a personas, organizaciones e instituciones. La prevención, la formación y la cultura de seguridad adquieren un papel tan importante como la propia tecnología.

Los contenidos que integran esta obra no pretenden ofrecer respuestas definitivas, sino contribuir a comprender la ciberseguridad desde una perspectiva integral, donde convergen el Derecho, la gobernanza, la gestión del riesgo, los controles

técnicos y la cultura organizacional. Más que centrarse en la tecnología, la propuesta es una invitación a fortalecer la cultura de prevención y a comprender que la seguridad digital requiere la participación de todos.

La privacidad digital constituye un derecho; protegerla y preservar la seguridad es un deber compartido. Si al concluir esta lectura el lector encuentra razones para volver a estas páginas, reflexionar sobre sus propias prácticas y fortalecer su compromiso con la protección de la información, el propósito que dio origen a esta obra habrá sido plenamente alcanzado.

PRÓLOGO

La acelerada transformación de los ecosistemas tecnológicos contemporáneos ha colocado a nuestras sociedades e instituciones frente a un dilema que trasciende con creces la ingeniería informática convencional. En la transición hacia entornos de interacción caracterizados por la convergencia de la Inteligencia Artificial Extendida (IA+), la hiperconectividad, los modelos emergentes de la Industria 5.0 y 6.0 y la cibernética, las fronteras tradicionales del control perimetral se han difuminado. Concebir la seguridad digital como una simple superposición de barreras técnicas o actualizaciones de software resulta una aproximación parcial, pues deja fuera la complejidad de los entornos sociotécnicos actuales: los ecosistemas informáticos contemporáneos son, en esencia, sistemas adaptativos complejos donde la tecnología, el marco normativo, los modelos de gobernanza y la conducta humana interactúan en bucles permanentes de retroalimentación.

Desde esta perspectiva sistémica, la seguridad y la resiliencia no emergen por decreto tecnológico, sino a través de una arquitectura de gobernanza capaz de regular la diversidad e incertidumbre del entorno digital. Es en este punto de inflexión donde la obra Ciberseguridad y Gobernanza en la Era Digital, concebida por la Dra. Carmen Carolina Ortega Hernández, adquiere una pertinencia y necesidad indiscutibles. Reconozco en la autora una trayectoria académica que articula el rigor computacional con la visión estratégica de la administración y el compromiso indeclinable

con el Derecho Digital. La labor desarrollada en la Benemérita Universidad Autónoma de Chiapas (UNACH) y su destacada presencia en cuerpos colegiados nacionales le otorgan autoridad para orientar el debate sobre la protección de nuestros activos intangibles en un momento histórico crucial.

La Dra. Ortega Hernández asume una postura intelectualmente lúcida: renuncia a las fórmulas mágicas y al determinismo tecnológico para tender un diálogo crítico y constructivo. La ciberseguridad se examina a lo largo de esta obra como un eje multidimensional donde convergen el marco jurídico, la gestión estratégica del riesgo, el rigor de los controles técnicos y, fundamentalmente, la cultura organizacional centrada en las personas. La autora desmonta el mito del usuario como simple eslabón vulnerable para reposicionarlo como el nodo neurálgico de conciencia, corresponsabilidad y soberanía cognitiva que sostiene la verdadera ciberdefensa.

Frente al rezago legislativo que aún experimenta México en materia de ciberseguridad, en este volumen la autora no solo expone las vulnerabilidades normativas e institucionales existentes, sino que propone una hoja de ruta orientada al fortalecimiento de políticas públicas, la adopción de modelos de madurez operativa y la tipificación de conductas ilícitas asociadas a tecnologías disruptivas. Asimismo, la obra destaca por su vocación formativa: desmitifica la complejidad computacional y provee una brújula indispensable para directivos, académicos, juristas y estudiantes comprometidos con la salvaguarda del ciberespacio.

En conclusión, Ciberseguridad y Gobernanza en la Era Digital es una contribución sustantiva que permite comprender cómo la preservación de la privacidad y seguridad de la información representan los cimientos de la soberanía de los datos y la seguridad digital en nuestro país. Por ello, invito a los lectores a adentrarse en estas páginas como quien consulta una guía estratégica para construir un provenir tecnológico más ético, seguro y resiliente.

Dr. Francisco Cervantes Pérez

Introducción General

En esta cruzada de innovación tecnológica, el internet continúa siendo un habilitador clave de la transformación digital. Las redes de alta velocidad, la computación distribuida, la nube y las tecnologías emergentes han creado ecosistemas digitales altamente conectados, pero también han incrementado los riesgos para la confidencialidad, integridad, disponibilidad y privacidad de la información. Esta realidad exige una visión integral de la ciberseguridad, en la que la protección tecnológica se complemente con estrategias de gobierno, procesos institucionales y participación responsable de las personas.

Desde esta perspectiva, la presente obra se estructura en tres capítulos que responden a las principales dimensiones de la ciberseguridad organizacional y que a su vez se vinculan con las tres líneas de generación del conocimiento (LGAC) del Programa de Estudio de la Maestría en Ciberseguridad Corporativa que oferta la Benemérita Universidad Autónoma de Chiapas,

Capítulo 1. Ciberseguridad Estratégica, Gobernanza y Gestión del Riesgo, su propósito es responder a la pregunta: ¿qué debe dirigir, gobernar y gestionar una organización para ser ciberresiliente?, proporcionando al lector una visión integral sobre los elementos que permiten fortalecer la capacidad de respuesta de las organizaciones frente a un entorno digital en constante evolución. El presente, tiene correspondencia con la LGAC *Gestión Estratégica de la Ciberseguridad, Gobernanza*

Digital y Riesgo Corporativo cuyo objetivo es diseñar políticas y marcos de gobernanza que alineen la mitigación del riesgo corporativo con los objetivos del negocio y las normativas vigentes.

Capítulo 2. Seguridad Técnica e Infraestructura Digital, su propósito es responder a la pregunta: ¿Cómo se protege técnicamente la infraestructura y los activos digitales?, a partir de esta interrogante, se presentan los principios, metodologías y tecnologías que actualmente constituyen la base para diseñar, implementar y fortalecer entornos digitales seguros en sistemas organizacionales públicos y privados. El presente, tiene correspondencia con la LGAC *Seguridad Técnica Avanzada, Infraestructura Digital y Tecnologías Emergentes*, orientada al desarrollo y optimización de tecnologías y mecanismos de protección para detectar vulnerabilidades y afrontar amenazas que puedan comprometer la ciberseguridad.

Capítulo 3. Cultura de Seguridad, Factor humano y Protección de Datos, su desarrollo responde a la pregunta: ¿Cómo lograr que las personas y las organizaciones adopten prácticas seguras de manera sostenible?, Esta interrogante, se plantea que la ciberseguridad no depende únicamente de la implementación de mecanismos de protección, sino también del compromiso de las instituciones para promover una cultura de seguridad orientada a la prevención y a la gestión responsable de los riesgos. En este sentido, la participación de las personas fortalece y mejoran las capacidades de protección frente a un entorno digital en constante evolución. Este capítulo tiene correspondencia con la LGAC *Cultura de Seguridad, Transformación Organizacional y Protección de Datos*, cuyo propósito es analizar el factor humano, la ética y la protección de datos personales en los procesos de adopción tecnológica, buscando desarrollar una cultura de seguridad que reduzca riesgos y promueva prácticas responsables en las organizaciones

En lo general, los tres capítulos permiten comprender que la ciberseguridad no depende de la tecnología, sino del equilibrio entre la estrategia institucional, los controles técnicos y el comportamiento responsable de las personas. En lo particular,

cada uno incorpora, al inicio, una descripción detallada de los elementos que lo integran, con el propósito de orientar al lector sobre los contenidos.

Posteriormente, se incluye un glosario organizado y clasificado de acuerdo con la función y las características de los conceptos que se desarrollan a lo largo de la obra. Entre ellos se encuentran la taxonomía de la ciberseguridad, la tríada de la ciberseguridad, los tipos de malware y las modalidades de ataques de infiltración mediante ingeniería social, entre otros conceptos relevantes.

Finalmente, como valor agregado a la obra, se incorporan anexos con información registrada como parte del seguimiento y sistematización del conocimiento generado, los cuales se presentan como una alternativa para favorecer su adopción y aplicación en contextos organizacionales.

Objetivo General

Analizar la ciberseguridad desde una perspectiva estratégica, técnica y humana, considerando la gobernanza, la gestión del riesgo, la protección de la infraestructura y los activos digitales, así como la cultura de seguridad y la protección de datos, con el propósito de contribuir al fortalecimiento de la Ciberresilencia y la adopción de prácticas seguras en las organizaciones.

Objetivos Específicos:

Capítulo 1. Ciberseguridad Estratégica, Gobernanza y Gestión del Riesgo,

- Analizar el marco jurídico mexicano aplicable al uso y adopción de las Tecnologías de Información y Comunicación, con énfasis en el desarrollo de software, la gestión de datos y los derechos y obligaciones relacionados con la ciberseguridad.
- Comparar las iniciativas legislativas en materia de ciberseguridad en México, identificando los ciberdelitos contemplados y aquellos asociados con tecnologías emergentes que permitan aportar elementos para una propuesta de ley federal de ciberseguridad.

- Proponer mecanismos de gestión del riesgo y controles basados en ISO/IEC 27001 que contribuyan al fortalecimiento de la gobernanza de la ciberseguridad y de la capacidad de respuesta de las organizaciones.

Capítulo 2. Seguridad Técnica e Infraestructura Digital

- Analizar los controles y buenas prácticas de seguridad aplicables a la infraestructura digital, con énfasis en la protección de bases de datos y activos digitales frente a las amenazas del entorno.
- Identificar vulnerabilidades y modalidades de ataque que pueden comprometer las bases de datos, plataformas digitales y dispositivos móviles, considerando mecanismos para su detección y prevención.
- Proponer medidas técnicas de mitigación del riesgo que contribuyan a fortalecer la protección de la infraestructura y los activos digitales en entornos organizacionales.

Capítulo 3. Cultura de Seguridad, Factor humano y Protección de Datos

- Analizar el papel del factor humano en la ciberseguridad, considerando la cultura de seguridad, la ética digital, la privacidad y la protección de datos personales.
- Examinar situaciones relacionadas con los riesgos derivados del comportamiento humano y la adopción tecnológica, mediante casos de análisis orientados al fortalecimiento de la cultura de ciberseguridad.
- Proponer políticas y buenas prácticas de seguridad informática que contribuyan al desarrollo de comportamientos responsables y a la reducción sostenible de los riesgos asociados al factor humano.

Capítulo 1.

Ciberseguridad Estratégica, Gobernanza y Gestión del Riesgo

Introducción

La ciberseguridad ha dejado de concebirse como un conjunto de controles tecnológicos para consolidarse como un factor transversal que fortalece la dirección estratégica, la gobernanza digital y la gestión integral del riesgo (Umaña & Turcio Alvarenga, 2024). Las amenazas también han evolucionado; se han vuelto más sofisticadas y letales desde su concepción hasta su ejecución, incorporando incluso herramientas basadas en inteligencia artificial que incrementan su alcance y capacidad de impacto.

En este contexto, las organizaciones públicas y privadas enfrentan un entorno cada vez más complejo, donde la continuidad de las operaciones, la protección de los activos digitales y el cumplimiento normativo dependen de su capacidad para anticipar riesgos y establecer mecanismos efectivos de gobierno. En consecuencia, la alta dirección debe asumir un papel proactivo en la definición de políticas, estrategias, modelos de gestión y estructuras de decisión que fortalezcan la resiliencia organizacional frente a los desafíos que plantea la transformación digital (Jacome, 2026).

Este capítulo desarrolla los fundamentos de la ciberseguridad estratégica desde una perspectiva de cumplimiento regulatorio, gobernanza digital y gestión del riesgo, presentando un análisis exploratorio del marco jurídico mexicano aplicable al uso y adopción de las Tecnologías de información y comunicación con énfasis en el desarrollo de software y gestión de datos en el marco de los derechos y obligaciones constitucionales, y una análisis comparativo de las iniciativas de ley en materia de ciberseguridad en México. Como propuesta de valor incluye un catálogo integrado por ciberdelitos definidos en iniciativas legislativas, y una aportación de ciberdelitos asociados a tecnologías emergentes, para una ley federal de ciberseguridad.

Así también, comparte un plan de administración de riesgo y un modelo para el sistema de gestión ISO 27001. La aplicación sistemática de estos controles permite fortalecer la gobernanza de la ciberseguridad al integrar medidas preventivas, detectivas y correctivas dentro de los procesos organizacionales.

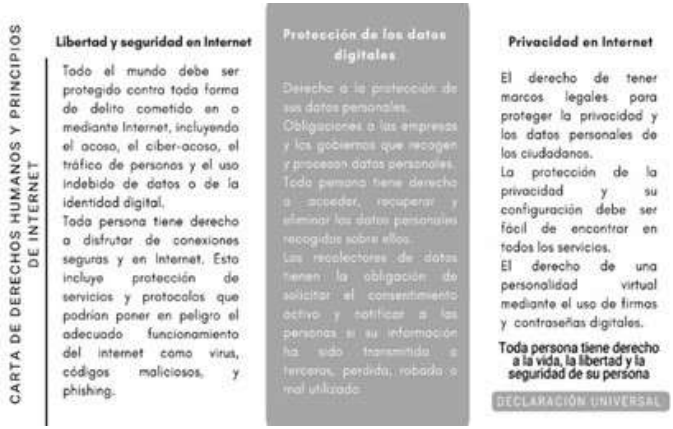
Hacia una Ley Federal de Ciberseguridad

El marco jurídico mexicano carece actualmente de un ordenamiento en materia de ciberseguridad que penalice las conductas ilícitas derivadas de la vertiginosa incorporación de las tecnologías de información y la comunicación al modelo social. Este hecho ofrece un entorno digital fértil para las amenazas digitales que cada día encuentran nuevas formas de vulnerar los protocolos de seguridad de los sistemas de información y recursos de telecomunicación, lo cual amplía la brecha tecnológica existente entre el Derecho Digital y la Seguridad Informática.

La ciberseguridad comprende el conjunto de políticas, procesos, controles, tecnologías y buenas prácticas orientadas a proteger a las personas, la información, los sistemas, las redes, los dispositivos y demás activos digitales frente a amenazas provenientes del ciberespacio. -*véase en glosario taxonomía de ciberseguridad*-. Su alcance trasciende la protección de la infraestructura tecnológica, al incorporar aspectos relacionados con la

gobernanza, la gestión del riesgo, la continuidad operativa, la resiliencia organizacional y el cumplimiento del marco jurídico aplicable (México, 2017).

Figura 1. Carta de derechos humanos y principios de Internet



Las innovaciones tecnológicas surgen en respuesta a la demanda digital de una sociedad denominada “del conocimiento”, que evoluciona acorde a los avances de la industria 5.0 y redes 5G, ofreciendo nuevas alternativas de servicios y productos, desarrollados principalmente sobre la base de sistemas expertos, inteligencia artificial, redes neuronales, robótica, ciencia de datos, internet de la cosas y computación en la nube. Sin embargo, debido al nivel de competitividad, estas tecnologías incursionan en el mercado con un grado de seguridad básico que se fortalece conforme evolucionan las amenazas y se actualizan los productos; esto expone a los usuarios a un escenario con vulnerabilidades que atenta contra los derechos humanos en materia de navegación segura, protección de datos y privacidad de la información.

Estos principios son reconocidos en la Carta de Derechos Humanos y Principios para Internet, para promover la seguridad, libertad, privacidad y confidencialidad en ambientes digitales

(ver figura 1); así como las obligaciones que deben cumplir los responsables de los datos personales de terceros y los derechos de sus titulares (CDHPI, 2015).

De la misma manera, la Constitución Mexicana (CPEUM, 2026) vigila el derecho a la información mediante la garantía de acceso a las tecnologías de la información y la comunicación, incluyendo Internet, conforme al artículo 6º, asimismo, protege la privacidad y los datos personales a través del artículo 16º, estableciendo el fundamento constitucional para la protección de la información y el respeto a la privacidad digital en el entorno tecnológico (ver figura 2).

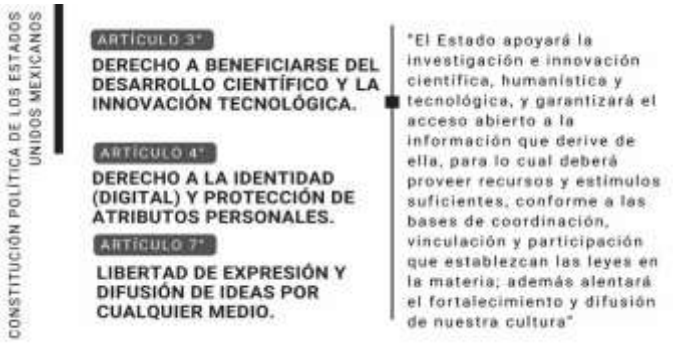
Figura 2. El derecho a la información y el derecho a la privacidad



Además, incorpora diversos derechos fundamentales que encuentran una estrecha relación con el entorno digital. El artículo 3º reconoce el derecho de toda persona a gozar de los beneficios del desarrollo de la ciencia, la tecnología y la innovación; el artículo 4º protege el derecho a la identidad, cuya acreditación actualmente se materializa también mediante mecanismos digitales. El artículo 7º tutela la libertad de expresión y difusión de ideas por cualquier medio (ver figura 3).

Asimismo, el artículo 28º salvaguarda los derechos de autor y los privilegios otorgados a los creadores de obras e innovaciones. Este precepto adquiere especial relevancia al respaldar la protección jurídica del software, los desarrollos tecnológicos, las innovaciones y demás activos intangibles que forman parte del patrimonio digital de las organizaciones.

Figura 3. Derecho de identidad digital y libertad de expresión



Aunque la Constitución no regula de manera expresa la ciberseguridad, sí establece un conjunto de derechos fundamentales que constituyen el sustento jurídico para el desarrollo de políticas públicas orientadas a la protección de la información, la privacidad, la identidad digital, el acceso a Internet, la innovación tecnológica y la seguridad de las personas en el ciberespacio.

En complemento a este marco constitucional, los delitos informáticos que vulneran estos derechos se encuentran sancionados por el Título Noveno del Código Penal Federal (CPF, Código Penal Federal, Revelación de secretos y acceso ilícito a sistemas y equipos de informática, 2026), relativo a la revelación de secretos y al acceso ilícito a sistemas y equipos de informática, particularmente en los artículos 210 y 211 Bis 1 al 211 Bis 7, los cuales establecen las conductas punibles y las sanciones aplicables (ver figura 4).

Figura 4. Revelación de secretos y acceso ilícito



Marco jurídico mexicano aplicable a las tecnologías de la información, la transformación digital y la ciberseguridad

En este apartado se presentan diversas disposiciones jurídicas publicadas en el Diario Oficial de la Federación, que incluyen artículos en relación a la definición de derechos, obligaciones, responsabilidades y procedimientos aplicables a las actividades que involucran el uso de las tecnologías de la información y la comunicación, la transformación digital, las transacciones electrónicas, la investigación de los delitos informáticos y el desarrollo científico y tecnológico (Ortega, Velasco, & López, 2023) (ver tabla 1).

Tabla 1. Marco jurídico mexicano aplicable a las tecnologías de la información, la transformación digital y la ciberseguridad.

No.	Ley / Código	Artículo	Obligación o disposición relevante
1	Ley de General de Educación (LGE, 2019)	16-VII	Educación inclusiva considerando las diversas capacidades, necesidades, estilos y ritmos de aprendizaje.
		18-III	Incorporación del conocimiento tecnológico mediante el uso de las tecnologías de la información, comunicación, conocimiento y aprendizaje digital.
		35 - IV	Reconocimiento de la educación abierta y a distancia como modalidad educativa.
		52-IV	Impulso al desarrollo tecnológico e innovación educativa mediante plataformas digitales de acceso abierto.
2	Ley de General de Educación Superior (LGES, 2021)	37-III	Promoción de la inclusión de personas con discapacidad en todos los tipos y modalidades educativas.
		37-IX	Impulso al acceso abierto a servicios informativos y repositorios mediante tecnologías digitales.
		44	Fortalecimiento de los modelos pedagógicos mediante tecnologías digitales e incorporación de competencias digitales en los planes de estudio.
3	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO, 2025)	17	Medidas necesarias para mantener exactos los datos personales.
		18	Procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.
		21-22	Aviso de privacidad integral y simplificado.
		24-27	Implementar mecanismos y medidas de seguridad administrativas y técnicas.
		29-30	Implementar sistema de gestión de las medidas de seguridad.
		37-40	Derechos ARCO (Acceso, Rectificación, Cancelación y Oposición).
		53	Relación del responsable y la persona encargada —contrato sobre el tratamiento de datos—.
		74-76	Responsabilidades para el administrador de la BD.

4	Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP, 2025)	7	Obtención lícita de datos personales sin medios fraudulentos.
		8	No podrán crearse base de datos con información personal sensible, sin justificación legítima.
		9	Consentimiento para el tratamiento de datos personales.
		16	Obligación de poner a disposición el Aviso de Privacidad.
		19	Implementación de medidas de seguridad administrativas, técnicas y físicas para proteger los datos personales.
		20	Las medidas deben ser proporcionales al tipo de datos y al riesgo del tratamiento
		21-26	Derecho ARCO
		62-63	Constituye infracción y 5 años en prisión incumplir el deber de seguridad de la BD y tratamiento de datos mediante engaño.
5	Ley Federal de Transparencia y Acceso a la Información (LFTAIP, 2024)	9-16	Responsabilidades de los Sujetos Obligados.
		21	Promoción de la transparencia, digitalización de la información pública y utilización de tecnologías de la información.
6	Ley General de Transparencia y Acceso a la Información Pública. (LGTAIP, 2025)	2-7	Promover la cultura de la transparencia en el ejercicio de la función pública, acceso a la información, participación ciudadana, así como la rendición de cuentas, mediante políticas públicas y mecanismos.
		44-46	Gestión de la Plataforma Nacional de Transparencia.
7	Ley General para la Inclusión de las Personas con Discapacidad (LGIPD, 2024)	4	Garantía de igualdad y no discriminación para las personas con discapacidad.
		12 II y IV	Promoción de la educación inclusiva, accesibilidad tecnológica y apoyos técnicos especializados.
8	Ley de Instituciones de Crédito Federal (LIC, 2024)	52	Uso de firma electrónica y mecanismos de autenticación para operaciones financieras mediante medios electrónicos.
9	Ley de Protección y Defensa al Usuario de Servicios Financieros (LPDUSF, 2024)	5	Protección y defensa de los derechos de los usuarios frente a las instituciones financieras.

10	Ley Federal de Protección al Consumidor, (LFPC, 2023)	76 bis	Protección de los consumidores en transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología.
11	Ley General de Títulos y Operaciones de Crédito (LGTOC, 2024)	12	Validez y efectos jurídicos de firmas y títulos de crédito.
		42	Procedimiento aplicable al robo, extravío o cancelación de títulos nominativos.
12	Ley Federal de Derecho de Autor (LFDA, 2020)	1,8,11, 20, 25, 29	Protección de los derechos morales y patrimoniales de los autores, sobre la propiedad intelectual, a partir de la impresión en un soporte material físico o digital.
		13 y 14 102,107 y 109	Protección de programas de cómputo, bases de datos y demás obras intelectuales, derechos y limitaciones.
		57- 84	Reconocimiento de la autoría y derechos patrimoniales derivados de la relación laboral.
		113-114	Responsabilidad de los proveedores de servicios de Internet respecto de contenidos digitales y procedimiento de aviso y retiro.
		152	Uso de obras pertenecientes al dominio público.
13	Ley Federal de Protección a la Propiedad Intelectual (LFPPI, 2020)	5-1	Protección de patentes, modelos de utilidad, diseños industriales, marcas y demás derechos de propiedad industrial.
14	Ley Federal del Trabajo (LFT, 2025)	330-A	Reconocimiento jurídico del teletrabajo mediante el uso de tecnologías digitales.
		330-I	Protección de la privacidad y de los datos personales durante el teletrabajo
		330-J	Obligaciones en materia de seguridad y salud para el trabajo a distancia.
15	Ley Federal de Telecomunicaciones y Radiodifusión (LFTR, 2024)	124	Interconexión e interoperabilidad de redes públicas de telecomunicaciones.
		125	Obligación de interconexión en condiciones objetivas y no discriminatorias.
		190 bis	Prohibición del uso de dispositivos inhibidores de señales de telecomunicaciones.
16	Ley de Aviación Civil (LAC, 2023)	30	Registro y regulación de aeronaves no tripuladas y dispositivos aéreos sujetos a control administrativo.

17	Ley General de Acceso de las Mujeres a una Vida Libre de Violencia (LGAMVLV, 2024)	5 IV	Definición de violencia contra las mujeres.
		6 V	Definición de violencia sexual.
		20-Quáter	Tipificación de la violencia digital
		20-Quinquies	Tipificación de la violencia mediática.
		20-sexies	Obligación de retirar contenido digital relacionado con violencia contra las mujeres.
18	Ley de Firma Electrónica Avanzada (LFEA, 2021)	2	Reconoce la firma electrónica avanzada como medio de identificación electrónica con efectos jurídicos.
		7	Establece que la firma electrónica avanzada produce los mismos efectos jurídicos que la firma autógrafa cuando cumple los requisitos previstos en la ley.
		8	Define los principios que deben cumplir los certificados digitales y la firma electrónica avanzada para garantizar autenticidad, integridad, confidencialidad y no repudio.
		13	Regula el uso de certificados digitales emitidos por Prestadores de Servicios de Certificación.
19	Código de Comercio(CC, 2024)	89	Reconocimiento jurídico de los mensajes de datos, la firma electrónica y el principio de neutralidad tecnológica.
		96	Validez jurídica de los métodos para crear firmas electrónicas
20	Ley para Regular las Instituciones de Tecnología Financiera (LRITF, 2024)	22-29	Requisitos funcionales para Instituciones de Fondos de Pago Electrónico.
		30-34	Operación con activos virtuales y definición de sus riesgos.
		47 y 56	Uso autorizado de tecnologías de información, redes de comunicación y medios de autenticación.
		68	Suspensión o revocación de autorización por deficiencias en infraestructura o controles.
		34	Los activos virtuales no constituyen moneda de curso legal ni cuentan con respaldo del Gobierno Federal o del Banco de México.

21	Ley General del Sistema Nacional de Seguridad Pública (LGSNSP, 2024)	2	Establece las bases de coordinación entre la Federación, las entidades federativas y los municipios para garantizar la seguridad pública.
		5	Define los fines de la seguridad pública, incluyendo la prevención de los delitos, su investigación y la sanción de las infracciones administrativas.
22	Ley General de Archivos (LGA, 2018)	4	Define conceptos fundamentales relacionados con documentos de archivo, documentos electrónicos, conservación y gestión documental.
		10	Obliga a los sujetos obligados a administrar, organizar y conservar los documentos que producen, reciben u obtienen en el ejercicio de sus funciones.
		42	Establece la preservación de los documentos de archivo electrónicos mediante medidas que garanticen su autenticidad, integridad, disponibilidad y conservación a largo plazo.
23	Ley General en Materia de Humanidades, Ciencias, Tecnologías e Innovación (LGHCTI, 2023)	5	Establece que las actividades de investigación, desarrollo tecnológico e innovación deberán realizarse bajo principios de responsabilidad ética, social y de seguridad, conforme a la normativa aplicable.
		11-XVII	Promueve el gobierno y la ciudadanía digitales mediante el desarrollo e implementación de tecnologías de la información, software libre y código abierto para fortalecer los servicios públicos.
		11-XXI	Impulsa el acceso abierto y gratuito mediante plataformas digitales a la información derivada de la investigación financiada por el Estado, respetando la información confidencial o reservada conforme a la legislación aplicable.
24	Código Penal Federal (CPF, Código Penal Federal, Revelación de secretos y acceso ilícito a sistemas y equipos de informática, 2026)	210	Sanciona la revelación ilícita de secretos cuando se afecte información protegida por disposición legal.
		211 bis 1 al 211 bis 7	Tipifica y sanciona el acceso ilícito a sistemas y equipos de informática, así como diversas conductas relacionadas con la afectación de la información y de la infraestructura informática.

Nota. *Las disposiciones descritas constituyen una síntesis elaborada por la autora a partir de los ordenamientos jurídicos vigentes. En todos los casos se cita el artículo correspondiente para facilitar su consulta en la fuente oficial.*

Asimismo, existen disposiciones administrativas y técnicas que fortalecen la regulación del uso de las tecnologías de la información. Entre ellas se mencionan:

- Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal (CEDN, 2021). Este acuer-do establece políticas para la gestión de las tecnologías de la información, la implementación de mecanismos de autenticación, el uso de certificados digitales, el desarrollo seguro de software, la protección de la información y la adopción de controles de seguridad informática en las dependencias y entidades de la Administración Pública Federal.
- Y en materia de aeronaves pilotadas a distancia, la Circular Obligatoria AV-23/10 R4 (DGAC, 2017) que establece las disposiciones técnicas para la operación de sistemas de aeronaves no tripuladas (RPAS), incluyendo requisitos relacionados con la seguridad operacional, restricciones de vuelo, protección de terceros y responsabilidades de los operadores, constituyendo un referente regulatorio para el empleo seguro de estas tecnologías.

La revisión de estos ordenamientos permite advertir que, pese a la existencia de diversos ordenamientos relacionados con las tecnologías de la información, la protección de datos, la firma electrónica, las transacciones digitales y los delitos informáticos, México aún carece de una ley de ciberseguridad que regule de manera integral esta materia.

Análisis comparativo del contenido de las iniciativas de ley en materia de ciberseguridad

Ante la ausencia de una ley federal de ciberseguridad vigente en México, diversos legisladores han presentado iniciativas con proyecto de decreto en materia de ciberseguridad, con fundamento en el artículo 71, fracción II de la Constitución Política de los Estados Unidos Mexicanos (CPEUM, 2026); con esto buscan establecer un marco jurídico especializado para regular la protección del ciberespacio, la prevención de los ciberdelitos y la seguridad de las infraestructuras digitales.

Con el propósito de identificar sus coincidencias, diferencias y alcances, se realizó un análisis comparativo considerando las principales dimensiones jurídicas, institucionales, técnicas y operativas incorporadas en cada propuesta (ver tabla 2).

Tabla 2. Iniciativas de ley en materia de ciberseguridad.

No.	Nombre de iniciativa	Legislador promovente	Fecha de presentación	Aporte principal
1	Ley de Ciberseguridad para la Ciudad de México (Von Roehrich de la Isla, 2020)	Christian Damián Von Roehrich De la Isla	27-10-2020	Seguridad pública y delitos
2	Ley General de Ciberseguridad (Mancera Espinosa, 2020)	Miguel Ángel Mancera Espinosa	01-09-2020	Infraestructura crítica
3	Ley General de Ciberseguridad (Guerra Mena, 2022)	Juanita Guerra Mena	03-10-2022	Coordinación institucional
4	Ley General de Ciberseguridad Ciudadana (Trasviña Waldenrath, 2024)	Jesús Lucía Trasviña Waldenrath	10-12-2024	IA, Sandbox, derechos
5	Ley Federal de Ciberseguridad (López Casarín, 2024)	Javier Joaquín López Casarín	20-03-2024	Educación y gobernanza
6	Ley Federal de Ciberseguridad y Confianza digital (Soto Ruíz, 2024)	Alejandra Lagunes Soto Ruíz	04-08-2024	Confianza digital, ética y desinformación

Nota: *El aporte principal constituye una interpretación elaborada por la autora a partir del análisis de cada iniciativa presentada ante el Congreso de la Unión.*

En el análisis comparativo se observa una evolución progresiva en el contenido de las propuestas legislativas. Las primeras iniciativas concentran su atención en la protección de la infraestructura tecnológica, la definición de competencias institucionales y la tipificación de los delitos informáticos.

Posteriormente, se incorporan temas relacionados con la coordinación entre autoridades, la protección de infraestructuras críticas y la gestión de riesgos. Y al final, las iniciativas más recientes amplían el alcance regulatorio al integrar aspectos como la gobernanza digital, la confianza digital, la inteligencia artificial, las tecnologías emergentes, la interoperabilidad, la protección de los derechos humanos y la educación en ciberseguridad (ver figura 5).

Figura 5. Evolución de las iniciativas de ley federal de ciberseguridad en México.



A partir del análisis de estas iniciativas se construyó una matriz comparativa que permite identificar la presencia de los principales elementos regulatorios incorporados en cada proyecto de decreto (ver tabla 3). Por razones de espacio, se presenta una versión sintética de la matriz, mientras que el análisis comparativo en extenso se puede consultarse en el Anexo 1. Matriz completa de las iniciativas de Ley de Ciberseguridad en México.

Tabla 3. Matriz comparativa de las iniciativas en materia de ciberseguridad en México, por dimensión de análisis.

No.	Dimensión	1	2	3	4	5	6
Gobernanza y organización institucional							
1	Principios generales	Sí	Sí	Sí	Sí	Sí	Sí
2	Creación de un órgano o autoridad nacional	Sí	Sí	Sí	Sí	Sí	Sí
3	Participación de la Secretaría de Seguridad, Fiscalía y órganos de representación	Sí	Sí	Sí	Sí	Sí	Sí
4	Cooperación nacional e internacional	Sí	Sí	Sí	Sí	Sí	Sí
Protección de Activos e Infraestructura							
5	Infraestructura crítica del Estado	Sí	Sí	Sí	Sí	Sí	Sí
6	Redes y sistemas de comunicación	Sí	Sí	Sí	Sí	Sí	Sí
7	Privacidad de la información	Sí	Sí	Sí	Sí	Sí	Sí
8	Protección de datos personales	Sí	Sí	Sí	Sí	Sí	Sí
Gestión de la ciberseguridad							
9	Políticas de ciberseguridad	Sí	Sí	Sí	Sí	Sí	Sí
10	Gestión del riesgo y continuidad operativa	Sí	Sí	Sí	Sí	Sí	Sí
11	Gestión de incidentes de ciberseguridad		Sí	Sí	Sí	Sí	Sí
12	Cultura y concientización en ciberseguridad			Sí	Sí	Sí	Sí
13	Educación y formación especializada			Sí	Sí	Sí	Sí
14	Certificación de especialistas	Sí	Sí	Sí			
Prevención, investigación y sanción							
15	Delitos informáticos	Sí	Sí	Sí	Sí	Sí	Sí
16	Penas y multas	Sí	Sí		Sí	Sí	Sí
17	Sanciones a servidores públicos y especialistas				Sí	Sí	Sí

Innovación y Transformación Digital							
18	Inteligencia artificial				Sí		Sí
19	Tecnologías emergentes				Sí		Sí
20	Confianza digital				Sí		Sí
21	Interoperabilidad				Sí		Sí
22	Sandbox regulatorio				Sí		Sí
23	Protección de derechos humanos en entorno digital				Sí	Sí	Sí
24	Ética digital						Sí
25	Desinformación						Sí

Nota: La presencia del (Sí) indica la incidencia de cumplimiento de la iniciativa por dimensión analizada.

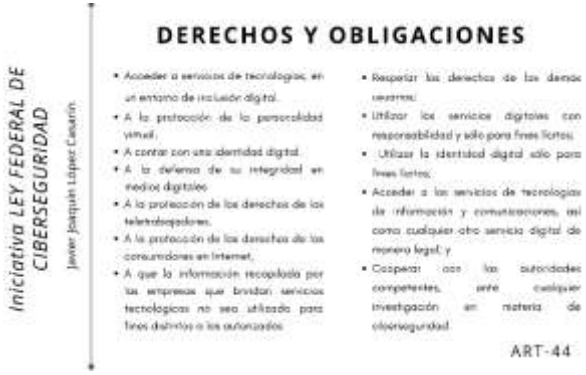
Del análisis comparativo de las iniciativas se identifican diversas coincidencias que evidencian un consenso legislativo respecto a los elementos mínimos que debe contener una futura ley federal de ciberseguridad. Entre las principales similitudes destacan las siguientes:

- Creación de un órgano rector con funciones para coordinar la política de ciberseguridad, la gestión del riesgo y la continuidad de las operaciones críticas, mediante un consejo o comisión.
- Colaboración con instituciones representantes del Estado, en materia jurisdiccional y administrativa, tales como: Fiscalía, Secretaría de Seguridad Pública, Secretaría de la Defensa Nacional, Secretaría de la Marina, entre otros, para fortalecer la coordinación interinstitucional.
- Armonización de la Ley con otros ordenamientos jurídicos, entre ellos: la Constitución Política de los Estados Unidos Mexicanos, Ley General del Sistema Nacional de Seguridad Pública, Ley de Protección de Datos, Ley de Derechos de Autor, Ley de Transparencia y Acceso a la Información, entre otros.

- Implementación de políticas y estrategias; así también, mecanismos de gestión del riesgo para prevenir, detectar, responder y recuperar la operación ante incidentes de ciberseguridad
- Fortalecimiento de una cultura de ciberseguridad, mediante acciones de capacitación, concientización y formación especializada.
- Concentración de especialistas, para capacitación en actividades de prevención, investigación, atención de incidentes y asesoría técnica.

Como un elemento diferenciador, la iniciativa de Ley presentada por Javier Joaquín López Casarín incorpora un catálogo de derechos y obligaciones, ampliando el alcance de regulación para los sectores público y privado en materia de ciberseguridad (ver figura 6).

Figura 6. Derechos y obligaciones en la iniciativa de Ley Federal de Ciberseguridad presentada por Javier Joaquín López Casarín.



Por su parte, las principales diferencias entre las iniciativas se observan en el alcance de su regulación. Mientras las primeras propuestas se concentran en los delitos informáticos, las sanciones y las atribuciones de las autoridades, las más recientes incorporan

temas como la inteligencia artificial, las tecnologías emergentes, la confianza digital, la educación en ciberseguridad y la protección de los derechos humanos. Ahora bien, con el propósito de ejemplificar las diferencias en la técnica legislativa utilizada por las iniciativas analizadas, la siguiente tabla presenta el tratamiento jurídico del delito de usurpación de identidad (ver tabla 4).

Tabla 4. Tratamiento legislativo del delito de usurpación de identidad en las iniciativas en materia de ciberseguridad en México.

No.	Iniciativa	Art.	Descripción del delito	Régimen sancionador
1	Ley de Ciberseguridad para la Ciudad de México (Von Roehrich de la Isla, 2020)	Art 65	Se sanciona a quien utilice, sin autorización, privilegios, credenciales, nombres de usuario o contraseñas para acceder a información o a las tecnologías de la información y comunicación en posesión de las autoridades, con la finalidad de afectar el debido ejercicio de la función pública.	Prisión de 6 meses a 2 años y multa 100 a 500 UMA
2	Ley General de Ciberseguridad (Mancera Espinosa, 2020)	49	Suplantación de la identidad de una persona mediante información personal en formato digital para realizar actos con consecuencias jurídicas.	Prisión de 6 a 8 años y multa de 200 a 800 UMA.
3	Ley General de Ciberseguridad Ciudadana (Trasviña Waldenrath, 2024)	60	Apropiación de un medio de identificación digital para usurpar la identidad de otra persona con el propósito de causar daño u obtener un beneficio.	Prisión de 3 a 9 años y multa de 600 a 8,000 UMA.
3	Ley Federal de Ciberseguridad (López Casarín, 2024)	61	El que suplante la identidad o se apropie de un medio de identificación de otra persona con el propósito de realizar una conducta tipificada como delito.	Prisión de 5 a 20 años y multa de 1,000 a 20,000 UMA.
5	Ley Federal de Ciberseguridad y Confianza Digital (Soto Ruíz, 2024)	54	Tipifica la usurpación de identidad dentro de los delitos previstos por la iniciativa.	Aplicar el Código penal

Nota: La descripción del delito no es una transcripción, si no una interpretación elaborada por la autora a partir del análisis de cada iniciativa presentada ante el Congreso de la Unión.

Como puede observarse, las iniciativas que consideran la usurpación de identidad como delito que debe ser sancionado, lo regulan con penas y sanciones aplicables diferentes, evidenciando la necesidad de homologar la tipificación en una ley federal.

Adicionalmente, se analizan las propuestas de reforma a la Ley de Seguridad Nacional presentadas por María Eugenia Hernández Pérez, María del Rocío Corona Nakamura y Cecilia Pinedo Alonso, orientadas a fortalecer la protección del Estado frente a riesgos digitales que pueden comprometer infraestructura crítica, redes de comunicación y sistemas de información. De ahí la necesidad de robustecer el marco jurídico para salvaguardar la privacidad, los datos personales y los sistemas frente a filtraciones, espionaje y otros ataques informáticos.

A continuación, se presenta una síntesis de las principales propuestas de reforma en materia de seguridad nacional relacionadas con la ciberseguridad (ver tabla 5).

El contenido comparativo detallado de las cinco iniciativas se incluye en el *Anexo 2. Matriz completa de las iniciativas de reforma a la Ley de Seguridad Nacional de México*.

Tabla 5. Iniciativas de reforma de la Ley de Seguridad Nacional de México.

Iniciativa	Aporte principal
Olga Juliana Elizondo Guerra (7 de abril del 2026)	Refuerza la protección de los sistemas informáticos y las bases de datos del Estado, al considerar como amenaza a la seguridad nacional las acciones dirigidas a sustraer, dañar, controlar, espiar, inhabilitar o interferir en el funcionamiento de los sistemas y redes informáticas de las instituciones y entidades estratégicas.
María del Rocío Corona Nakamura (3 de agosto de 2022)	Incorpora una definición amplia de amenaza cibernética al reconocer que cualquier acto, incidente o conducta maliciosa proveniente del ciberespacio puede afectar a las personas, la información, los activos digitales, las tecnologías de operación y las instituciones del Estado.
María Eugenia Hernández Pérez (11 de octubre de 2022)	Fortalece la protección de la infraestructura crítica del Estado, incorporando una definición jurídica de ciberespacio y vinculando las amenazas digitales con la integridad de los datos, los sistemas de información y la actuación del Consejo de Seguridad Nacional en el resguardo de información estratégica.
Cora Cecilia Pinedo Alonso (7 de diciembre de 2022)	Introduce un enfoque integral de ciberseguridad, al definir jurídicamente el concepto de *ciberseguridad* e incorporar elementos como políticas, gestión del riesgo, formación, buenas prácticas, tecnologías y medidas de protección aplicables tanto al sector público como al privado.
Miguel Ángel Mancera Espinosa (1 de septiembre de 2020)	Protege la infraestructura de telecomunicaciones como activo estratégico, al considerar amenaza a la seguridad nacional cualquier acto que afecte las redes e infraestructura indispensables para la prestación de servicios públicos y el funcionamiento del Estado.

Nota. El aporte principal constituye una interpretación elaborada por la autora a partir del análisis de cada iniciativa y aportación al desarrollo del marco jurídico en materia de ciberseguridad presentadas ante el Congreso de la Unión. Al cierre de la presente obra, algunas de ellas han sido desechadas o permanecen sin aprobación legislativa.

Propuesta de integración de un catálogo de ciberdelitos para una ley federal de ciberseguridad

La evolución acelerada de las tecnologías digitales ha propiciado la especialización de nuevas modalidades delictivas que afectan la seguridad de la información, la privacidad de los datos y el ejercicio de diversos derechos fundamentales. En contraste, el marco jurídico mexicano continúa enfrentando desafíos para responder con la misma rapidez a estos cambios tecnológicos, generando áreas de oportunidad que requieren una actualización normativa integral.

Con este antecedente, se propone integrar en un mismo marco jurídico los elementos más relevantes identificados en las iniciativas legislativas analizadas, con el propósito de consolidar una Ley de Ciberseguridad que fortalezca la protección jurídica en el ciberespacio.

Entre sus componentes, dicha ley debería incorporar un capítulo específico que concentre los ciberdelitos comunes, estableciendo una correspondencia entre los distintos tipos penales, su descripción, las sanciones aplicables y las disposiciones jurídicas relacionadas, evitando duplicidades y fortaleciendo la certeza jurídica.

En este sentido, la tabla 6 presenta una propuesta de integración de los ciberdelitos identificados en las distintas iniciativas legislativas analizadas, los cuales constituyen una propuesta base para estructurar un catálogo unificado de conductas sancionables a personas que orientan sus habilidades y conocimientos para vulnerar las medidas de seguridad -*véase glosario tipos de especialista en ciberseguridad*-.

Tabla 6. Propuesta de catálogo unificado de ciberdelitos.

No.	Ciberdelitos:
	Acceso ilícito
1	Intrusión a sistemas de información, aplicaciones, plataformas, sitios web o cualquier programa de procesamiento de datos.
2	Intrusión a equipos de cómputo, dispositivos móviles, dispositivos inteligentes o cualquier hardware para el procesamiento de datos.
3	Intrusión a medios de almacenamiento físico fijo, extraíble o portable.
4	Intrusión a servidores, antenas y repetidores o cualquier sistema de comunicación por red.
5	Intrusión a dispositivos y controladores de conexión entre dispositivos: Bluetooth, QR, IP, otros.
6	Interceptación de señales y mensajes, enviados por una conexión de punto a punto.
Ataques contra sistemas	
7	Diseño, desarrollo, reproducción, comercialización y/o arrendamiento de software y/o hardware malicioso que atenten contra la seguridad de las tecnologías de información y comunicación.
8	Modificación de software y/o hardware con fines maliciosos que atenten contra la seguridad de las tecnologías de información y comunicación.
Ataques contra la información	
10	Modificación, eliminación y/o reproducción de ficheros con datos personales, información privada y contenido digital, sin autorización del titular.
11	Modificación, eliminación y/o reproducción de ficheros que altera la integridad de la información pública con fines ilícitos.
12	Robo de información digital en sistemas de información y medios de almacenamiento electrónicos, físicos y en la nube, que altere confidencialidad de la información.
13	Espionaje digital, con actividad de vigilancia, monitoreo o inteligencia clandestina para obtener información confidencial.
Delitos contra la identidad	
14	Usurpación de la identidad digital de cuentas de correo, perfil de usuario, contraseñas, QR, firma electrónica (e-firma), tarjetas, token, NIP y *avatar*, que identifican al titular en medios electrónicos, web y virtuales.
15	Falsificación de documentos digitales y firma electrónica.

Delitos financieros	
16	Estafa o fraude digital mediante sitios web, plataformas, aplicaciones, redes sociales o entornos virtuales que simulen ser oficiales o legítimos, induciendo a la víctima, mediante engaño o manipulación, a realizar transacciones o proporcionar información con fines ilícitos.
17	Extorsión digital mediante el uso de tecnologías de la información, plataformas digitales, redes sociales, aplicaciones, servicios de mensajería o cualquier medio electrónico, utilizando amenazas, intimidación o coacción para obligar a la víctima a entregar dinero, bienes, información, credenciales de acceso o realizar cualquier acto en beneficio del agresor.
Delitos contra la propiedad intelectual	
18	Copia, modificación y/o reproducción de la propiedad intelectual en formato digital violando la protección que otorga el derecho de autor.
Delitos contra redes y telecomunicaciones	
19	Distribución, retransmisión o comercialización no autorizada de la señal de Internet o Wi-Fi, mediante la réplica o redistribución del servicio proporcionado por un concesionario o proveedor autorizado.
20	Obtención ilícita de acceso a una red inalámbrica (Wi-Fi) mediante el uso no autorizado del identificador de red (Service Set Identifier, SSID), contraseñas o cualquier otro mecanismo de autenticación, con el propósito de utilizar el servicio sin el consentimiento del titular
Contenido ilícito	
21	Distribución de contenido digital ilícito en sitios web, plataformas, aplicaciones y redes sociales.
22	Violencia digital y mediática.
23	Creación, modificación o reproducción de contenido digital mediante sistemas, software o herramientas basadas en inteligencia artificial que simulen la identidad, apariencia o voz de una persona con fines ilícitos.

Nota. La clasificación de los ciberdelitos constituye una propuesta de integración elaborada por la autora a partir del análisis comparativo de las iniciativas de reforma en materia de ciberseguridad presentadas ante el Congreso de la Unión. Las denominaciones y descripciones fueron homologadas para facilitar su análisis y no corresponden necesariamente a la redacción literal de las iniciativas.

Entre las conductas incorporadas en el catálogo propuesto de ciberdelitos se encuentra la violencia digital y mediática -*véase glosario tipos de violencia*-., cuya incidencia se ha incrementado como consecuencia del uso masivo de Internet, las redes sociales

y las plataformas digitales. Mientras la violencia digital comprende diversas conductas de acoso, hostigamiento, persecución, suplantación de identidad, difusión no autorizada de información y otras formas de agresión ejercidas mediante medios digitales, la violencia mediática se caracteriza por la difusión, publicación o reproducción masiva de contenidos que vulneran la dignidad, la intimidad, la seguridad o los derechos de las personas a través de medios de comunicación, plataformas digitales o redes sociales.

La violencia digital adopta distintas modalidades; su identificación permite comprender mejor las formas en que se ejerce la violencia y facilita el diseño de estrategias de prevención, atención y protección de las víctimas.

La figura 7 ilustra algunos tipos de violencia digital identificadas en el entorno digital por su denominación anglosajona.

Figura 7. Violencia digital y sexual digital.



En seguimiento, la tabla 7 presenta una descripción sintética de los tipos de violencia digital y su principal forma de afectación.

Tabla 7. Tipos de violencia digital.

No.	Violencia digital:	Descripción
1	Sex selfie	Desvelamiento de contenido sexual, violando los derechos de privacidad a la intimidad.
2	Gossip	Denigración digital a través de la difusión de rumores por Internet.
3	Stalking	Acecho y espionaje digital.
4	Ciberbullying	Discriminación y acoso digital.
5	Griefing	Agresión y acoso digital en videojuegos.
6	Doxing	Revelar información personal que identifica a una persona, para avergonzar o poner en riesgo.
7	Sexting	Acoso sexual digital.
8	Frexting	Acoso sexual digital entre contactos registrados.
9	Grooming	Acoso sexual digital infantil.
10	Cibertrolling	Provocación con amenazas e insultos en foros virtuales.
11	Happy slapping	Difusión de contenido digital sobre un acto de agresión física o verbal.
12	Sextorsión	Extorsión mediante contenido sexual para la explotación y chantaje sexual.
13	Ghosting, orbiting, zombing, benching, curving, haunting y cricketing	Violencia digital afectiva, sobre los tipos y formas de participación y omisión de actividad en línea.
14	Flexting, catfish	Falsificación de identidad digital.

La violencia digital sexual merece un tratamiento diferenciado debido a la afectación que produce sobre la intimidad, la dignidad, la libertad y el desarrollo de las personas. Su relevancia jurídica ha motivado la incorporación de mecanismos específicos de protección en la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia, en las reformas de la Ley Olimpia (LO, s.f.) y, en iniciativas legislativas que proponen sancionar el uso de sistemas y herramientas basadas en inteligencia artificial para la generación y difusión de contenido íntimo no consentido. La tabla 8 presenta algunos tipos de violencia digital sexual.

Tabla 8. Tipos de violencia digital sexual.

No.	Violencia digital sexual:	Descripción
1	Sex selfie	Difusión no autorizada de contenido íntimo generado por la propia víctima, vulnerando su privacidad e intimidad.
2	Sexting	Acoso sexual digital.
3	Frexting	Acoso sexual digital entre contactos registrados.
4	Grooming	Acoso sexual digital infantil.
5	Sextorsión	Extorsión mediante contenido sexual para la explotación y chantaje sexual.

La violencia mediática ha impulsado reformas legislativas a través de la Ley Ingrid (LI, s.f.), con el propósito de evitar la exposición de las personas ante medios para proteger la intimidad y dignidad de las víctimas y sus familiares. Con esto se combate la violencia mediática de género y su normalización y se sanciona a las personas que lo realicen.

Si bien la propuesta de catálogo unificado de ciberdelitos integra las principales conductas identificadas en las iniciativas legislativas analizadas, la rápida evolución tecnológica plantea un reto adicional para el legislador con la aparición de nuevos modelos de computación, activos digitales, mecanismos de autenticación, inteligencia artificial y entornos virtuales; dando origen a escenarios que evolucionan con mayor rapidez que los procesos de actualización normativa, por lo que resulta necesario anticipar nuevas conductas susceptibles de regulación.

En este contexto surge una interrogante que orienta la presente propuesta: *¿Qué ciberdelitos deberían incorporarse en una futura ley federal de ciberseguridad para responder a los riesgos asociados a las tecnologías emergentes?*

Con base en este planteamiento, se propone la incorporación de nuevas figuras delictivas asociadas a tecnologías emergentes, con el propósito de complementar el catálogo de ciberdelitos y fortalecer la capacidad del marco jurídico para responder a las amenazas presentes y futuras derivadas de la transformación digital (ver tabla 5).

Tabla 9. Propuesta de nuevos ciberdelitos asociados a tecnologías emergentes.

No.	Ciberdelitos:
	Computación distribuida
1	Intrusión a los sistemas de computación en la nube (cloud computing y edge computing).
	Blockchain y activos digitales
2	Diseño, desarrollo y/o reproducción de algoritmos de desencriptación, con fines maliciosos que atenten contra la seguridad de la criptografía en Blockchain.
3	Copia, modificación y/o reproducción de la propiedad industrial en formato digital, violando la protección que otorga el derecho exclusivo del titular.
	Propiedad intelectual e industrial digital
4	Robo de activos virtuales, criptomonedas y bitcoins.
	Identidad digital y biometría
5	Usurpación de la identidad biométrica mediante el uso no autorizado de huella digital, reconocimiento facial, retina, iris u otros mecanismos de autenticación biométrica.
6	Clonación de contenido digital de un dispositivo, sistema o cuenta electrónica, sin autorización del titular.
7	Alteración, bloqueo o manipulación ilícita de los mecanismos de interoperabilidad entre plataformas, aplicaciones, sistemas o servicios digitales, que impida o afec-te el intercambio de información o la continuidad de los servicios.
	Plataformas y servicios digitales
8	Alteración o manipulación ilícita de plataformas digitales y servicios de intermediación tecnológica, mediante técnicas automatizadas, algoritmos, bots o accesos no autorizados, con el propósito de modificar la disponibilidad, visibilidad, distribución o integridad de contenidos, servicios o información digital.
9	Alteración o manipulación ilícita de mecanismos de accesibilidad digital que impidan o restrinjan el acceso de personas con discapacidad o barreras de comunicación a plataformas, aplicaciones o servicios tecnológicos.
10	Desarrollo, reproducción o utilización de sistemas, software o herramientas basadas en inteligencia artificial, redes neuronales o tecnologías de autoaprendizaje, con fines maliciosos que atenten contra la seguridad de las personas, los sistemas de información o estabilidad del entorno digital.
11	Manipulación ilícita de mecanismos de búsqueda, posicionamiento o distribución digital para facilitar la descarga, propagación o difusión de software malicioso, aplicaciones fraudulentas o código dañino.

Inteligencia artificial	
12	Realización de acciones ilícitas mediante avatares, identidades virtuales o representaciones digitales en entornos inmersivos o metaversos, con el propósito de causar afectación física, psicológica, patrimonial o reputacional.
Tecnologías inmersivas	
13	Filtración, reproducción o difusión de contenido digital de una víctima derivado de actos de agresión física, psicológica o sexual, sin su consentimiento, con el propósito de causar daño, humillación o afectación a su dignidad.
14	Obtención, seguimiento, monitoreo o comercialización ilícita de datos de geolocalización de personas, dispositivos o medios de transporte, sin autorización del titular o mandato legal.
Internet de las cosas (IoT) y gemelos digitales	
15	Manipulación ilícita de dispositivos conectados a Internet de las Cosas (IoT), con el propósito de alterar su funcionamiento, comprometer la seguridad de las personas o afectar la prestación de servicios
16	Alteración, manipulación o reproducción ilícita de gemelos digitales utilizados para representar, controlar o supervisar procesos, infraestructuras o activos físicos, con el propósito de afectar su funcionamiento, integridad o disponibilidad.

Nota. Los ciberdelitos propuestos constituyen una propuesta elaborada por la autora a partir del análisis de las iniciativas legislativas y de los riesgos asociados a la transformación digital. Su incorporación en un futuro ordenamiento jurídico requeriría el correspondiente análisis técnico y legislativo.

La evolución de estas conductas evidencia que la protección del ciberespacio no depende exclusivamente de la implementación de controles tecnológicos. Si bien las medidas de seguridad informática permiten prevenir, detectar y mitigar riesgos, su eficacia debe complementarse con un marco jurídico que establezca derechos, obligaciones y responsabilidades para los distintos actores del entorno digital, así como mecanismos de prevención, investigación y sanción de las conductas ilícitas.

Si bien el fortalecimiento del marco jurídico constituye un componente esencial de la ciberseguridad, por sí solo resulta insuficiente. La protección del ciberespacio también requiere la adopción de modelos de gobernanza, gestión del riesgo y estándares internacionales que orienten la implementación de controles y buenas prácticas en las organizaciones. En este sentido, el siguiente apartado aborda el papel de las normas ISO como referente para la gestión integral de la ciberseguridad.

Gobernanza de las plataformas digitales: la experiencia europea DMA y DSA

El marco jurídico mexicano continua enfrentado desafíos para regular de manera integral diversas actividades digitales que se desarrollan en el ciberespacio, razón por la cual debemos seguir atentos a nuevas leyes internacionales que ofrecen esquemas regulatorios, que pueden servir como referencia para futuras adecuaciones normativas.

En ese sentido, la gobernanza de las plataformas digitales constituye uno de los componentes estratégicos de la ciberseguridad moderna, debido a que gran parte de la información, las comunicaciones y los servicios digitales dependen actualmente de ecosistemas administrados por proveedores tecnológicos. En consecuencia, la regulación de estas plataformas no solo persigue objetivos relacionados con la competencia económica o la protección de los consumidores, sino también el fortalecimiento de la seguridad de la información, la privacidad, la interoperabilidad y la confianza en el entorno digital. Entre la diversidad de leyes existente, dirigimos la atención a las siguientes:

- Ley de Mercados Digitales (DMA)

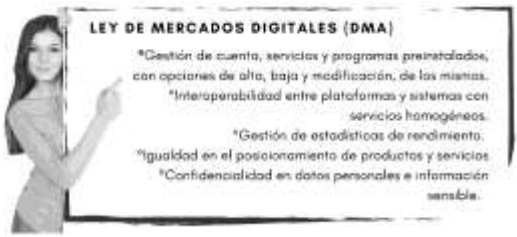
Es el ordenamiento legal europeo que entró en vigor el 7 de marzo de 2024, con el propósito de vigilar la actuación de las plataformas tecnológicas denominadas “guardianes del acceso digital” (gatekeepers), citando como ejemplo a Alphabet (Google), Amazon, Apple, ByteDance (TikTok), Meta y Microsoft, respecto a la asignación de términos y condiciones que aplican a otras empresas y consumidores de forma discrecional.

De esta manera se abre la posibilidad de permitir tiendas de aplicaciones de terceros en sus sistemas operativos, garantizar la interoperabilidad en servicios de mensajería y prohibir la priorización de sus propios servicios sobre los de sus competidores, con el fin de fomentar un entorno digital más justo y competitivo.

El posicionamiento de marca que tienen las plataformas líderes no debe ser factor para discriminar o limitar la actuación o crecimiento de otros modelos de negocios. La oferta de servicios

y productos debe estar sujeto a lineamientos que regulen sin distinción alguna la participación de todos en el entorno digital y garanticen la competencia leal por Internet; al mismo tiempo, contemplar multas que van de 10 % a 20 % del volumen total de negocios si esas regulaciones se incumplen. Entre algunos temas de regulación, se observan los siguientes (ver figura 8):

Figura 8. Ley de mercados digitales.



Por ejemplo, con el soporte del principio de interoperabilidad, se pretende aumentar la conectividad de los usuarios mediante la convivencia entre dispositivos inteligentes y algunas plataformas de comunicación, logrando con ello brindar el servicio de envío y recepción de mensajes instantáneo, en forma conjunta. Definitivamente, esta acción representa una nueva obligación que deberán asumir los proveedores de servicio, otorgando un beneficio a los usuarios acorde a las innovaciones tecnológicas en materia de protocolos de comunicación; sin embargo, las plataformas deberán fortalecer los mecanismos de seguridad para implementar un espacio seguro de interconexión digital (DMA, s.f.).

No obstante, desde la perspectiva de la ciberseguridad, la interoperabilidad también representa un reto para la seguridad de la información, ya que la interconexión entre plataformas incrementa la superficie de exposición a amenazas y exige la adopción de mecanismos de autenticación, cifrado, control de acceso y gestión del riesgo que garanticen la confidencialidad, integridad y disponibilidad de la información compartida entre los distintos servicios digitales

- Ley de Servicios Digitales

La Ley de Servicios Digitales (DSA) también es un nuevo marco legal europeo aprobado a mediados de 2022 que entró en vigor el 17 de febrero de 2024, con el fin de regular el contenido ilícito que se aloja en las plataformas digitales y motores de búsqueda y que es empleado como precursor de actos de violencia y delictivos (ver figura 9).

Figura 9. Ley de Servicios Digitales.



La responsabilidad del contenido ilícito no aplica a los proveedores de servicios, cuando se demuestre que fue retirado del ciberespacio inmediatamente después de su conocimiento y bloqueados los permisos de acceso, empleando estrategias de detección temprana.

En los casos en donde el contenido ilícito sea presentado por terceros a través de los servicios que ofrecen las plataformas, se da la exclusión de responsabilidad, toda vez que se avale la participación del usuario al cual se le hace responsable directo; previa identificación y rastreo en los términos legales. Existe la apertura para revocar la designación, siempre y cuando se lleve a cabo el procedimiento extrajudicial o judicial y se dictamine a favor del imputado. Desde la perspectiva de la ciberseguridad, la DSA fortalece la corresponsabilidad entre plataformas, usuarios y autoridades, promoviendo mecanismos de detección, notificación y respuesta frente al contenido ilícito, sin perder de vista el respeto a los derechos fundamentales y al debido proceso (DSA, s.f.).

Desde la perspectiva de la ciberseguridad, la DSA fortalece la corresponsabilidad entre plataformas, usuarios y autoridades mediante mecanismos de prevención, detección, notificación y respuesta frente al contenido ilícito. Asimismo, contribuye a la protección de la seguridad de la información, la privacidad, la identidad digital y otros derechos fundamentales, promoviendo un entorno digital más seguro y confiable sin menoscabo del debido proceso y las garantías jurídicas de los usuarios.

Gobernanza de la ciberseguridad y gestión del riesgo

La seguridad de la información constituye uno de los principales fundamentos de la ciberseguridad, sustentada en los principios de *confidencialidad, integridad y disponibilidad (CID),* que constituyen el fundamento de la seguridad de la información (Quadra-Salcedo & Piñar Mañas, 2018). La protección de estos atributos no depende únicamente de la implementación de controles tecnológicos, sino también de la capacidad de las organizaciones para establecer mecanismos de dirección, supervisión y mejora continua que permitan gestionar los riesgos asociados al uso de las tecnologías de la información.

En este contexto, la gobernanza de la ciberseguridad orienta la toma de decisiones estratégicas, alineando los objetivos institucionales, las políticas de seguridad, la gestión del riesgo y el cumplimiento del marco jurídico aplicable. Así también, comprende el conjunto de estructuras, políticas, procesos y responsabilidades mediante los cuales la organización dirige y supervisa la protección de sus activos digitales. Desde esta perspectiva, la ciberseguridad deja de ser también exclusiva del área de tecnologías de la información para convertirse en una responsabilidad compartida entre la alta dirección, las áreas operativas, los responsables de los procesos y las instancias encargadas del cumplimiento normativo y la gestión del riesgo.

En este sentido, el Institute of Internal Auditors (IIA) establece, en los Requisitos Temáticos de Ciberseguridad, que la gobernanza debe sustentarse en una estrategia formal, objetivos claramente definidos, políticas institucionales actualizadas,

funciones y responsabilidades claramente asignadas, así como en la participación activa de la alta dirección para supervisar el desempeño de la ciberseguridad y atender las amenazas emergentes. Asimismo, señala que la gestión del riesgo debe desarrollarse como un proceso permanente de identificación, análisis, tratamiento y seguimiento de los riesgos que puedan afectar el logro de los objetivos organizacionales (IIA, 2026).

Desde esta perspectiva, el liderazgo constituye uno de los pilares de la gobernanza. Corresponde a la alta dirección definir el nivel de riesgo aceptable para la organización, aprobar las políticas institucionales de seguridad, asignar los recursos humanos, tecnológicos y financieros necesarios, así como supervisar periódicamente la eficacia de los controles implementados. Su participación fortalece la capacidad institucional para anticipar amenazas, responder oportunamente a los incidentes y garantizar la continuidad de las operaciones.

La implementación de un sistema de gestión de seguridad de la información (SGSI) se materializa mediante políticas, procedimientos, controles y mecanismos de mejora continua que orientan el uso seguro de los recursos tecnológicos dentro de la organización. Bajo este enfoque, la gobernanza integra la estrategia institucional con la gestión del riesgo, permitiendo que las decisiones relacionadas con la ciberseguridad se fundamenten en criterios técnicos, organizacionales y normativos, lo cual fortalece la resiliencia y la continuidad operativa.

Una de las herramientas que materializa esta visión es el plan de administración del riesgo, instrumento que permite documen-tar de manera sistemática los riesgos identificados por software, bases de datos, hardware, redes, aplicaciones web, infraestruc-tura tecnológica, procedimientos, recursos humanos y recursos materiales, para detectar las vulnerabilidades existentes, las amenazas asociadas, la probabilidad de ocurrencia, el impacto esperado, el nivel de riesgo y las acciones preventivas y correctivas necesarias para reducir sus efectos sobre la organización (Ortega Hernández, 2014).

El plan también considera la inversión requerida y el costo asociado a la materialización del riesgo, elementos que permiten

valorar las consecuencias económicas de los escenarios identificados y sustentar la selección de las medidas de tratamiento.

Esta perspectiva encuentra respaldo en estudios realizados en México, como el *Estado de la Ciberseguridad en el Sistema Financiero Mexicano*, elaborado por la Organización de los Estados Americanos (OEA) con la participación de la Comisión Nacional Bancaria y de Valores (CNBV), que analiza indicadores relacionados con el presupuesto destinado a la seguridad digital, los costos de respuesta y recuperación ante incidentes, así como su relación con el tamaño y el sector de las entidades financieras.

Estos indicadores permiten dimensionar el impacto económico asociado a la materialización de los incidentes y constituyen un referente para incorporar la dimensión económica en la gestión del riesgo (OEA, 2019)

A continuación, se comparte un plan de administración del riesgo, con el propósito de facilitar su adaptación e implementación en distintos contextos organizacionales (ver tabla 10).

Tabla 10. Plan de administración del riesgo.

Dimensión	Software
Riesgo	Fallas durante actualizaciones o aplicación de parches
Vulnerabilidad	Software desactualizado
Amenaza	Ciberataques por exploits conocidos
Probabilidad	9
Impacto	9
Nivel del riesgo %	81
Acción preventiva	Implementar actualizaciones automáticas
Acción correctiva	Monitoreo constante y parches de emergencia
Inversión	*
Costo	*

Nota: El presente plan de administración del riesgo es un ejemplo correspondiente a la dimensión de Software.

1. *Dimensión.* Componente organizacional sujeto al análisis: software, hardware, redes, bases de datos, infraestructura, aplicaciones web, recursos humanos, entre otros.
2. *Riesgo.* Evento potencial que puede afectar el logro de los objetivos.
3. *Vulnerabilidad:* Debilidad susceptible de ser explotada por una amenaza.
4. *Amenaza.* Agente con capacidad de materializar una vulnerabilidad y provocar un incidente de seguridad.
5. *Probabilidad.* Estimación de la posibilidad de ocurrencia del riesgo valorada en una escala de 1(muy baja) a 10 (muy alta).
6. *Impacto.* Nivel de afectación que ocasionaría la materialización del riesgo, sobre las operaciones de la organización, valorada en una escala de 1 (mínimo) a 10 (crítico).
7. *Nivel del riesgo (%).* Resultado obtenido de multiplicar la probabilidad por el impacto, generando un valor del 1 al 100, que facilita la priorización de los riesgos para su tratamiento.
8. *Acción preventiva*: Controles orientados a disminuir o eliminar vulnerabilidades antes de que el riesgo se materialice.
9. *Acción correctiva*: Medidas destinadas a contener o recuperar la operación una vez ocurrido el incidente.
10. *Inversión*: Recursos económicos requeridos para implementar controles preventivos, adquirir tecnología o fortalecer las capacidades institucionales.
11. *Costo* por materialización del riesgo: estimación de las pérdidas económicas derivadas del incidente, incluyendo interrupción de operaciones, recuperación de la información, restauración de servicios, contratación de especialistas o peritos forenses, sanciones legales, afectaciones reputacionales y pérdida de clientes.

A manera de referencia, se presenta la siguiente matriz de riesgos por dimensión, con el propósito de considerarlo como *guía práctica* para su implementación de acuerdo con las necesidades de cada organización (ver tabla 11).

Tabla 11. Matriz de riesgos por dimensión.

Dimensión	***Riesgos***
Software	· Errores de programación · Vulnerabilidades en el código fuente. · Errores en los mecanismos de cifrado y encriptación de datos. · Uso de software no autorizado o sin licencia. · Configuración incorrecta de aplicaciones y controladores. · Exposición de información sensible. · Uso de versiones desactualizadas o sin soporte. · Fallas durante actualizaciones o aplicación de parches. · Incompatibilidad entre aplicaciones. · Configuración insegura de aplicaciones.
Base de datos	· Inyección SQL. · Accesos no autorizados. · Privilegios excesivos. · Configuración insegura del gestor de bases de datos. · Fugas de información. · Respaldos sin cifrado. · Ausencia de auditoría de transacciones. · Bases de datos desactualizadas. · Exposición de credenciales de conexión. · Pérdida o corrupción de la información.
Hardware	· Daño físico en computadores y servidores. · Sobrecalentamiento de equipos. · Robo o extracción de equipos. · Daño físico de discos duros o unidades de almacenamiento. · Fallas en dispositivos de almacenamiento. · Obsolescencia tecnológica. · Falta de mantenimiento preventivo. · Daños ocasionados por variaciones de energía eléctrica. · Falla de componentes críticos (memoria, fuente de poder, procesadores).

Redes	· Ataques de denegación de servicio (DoS/DDoS). · Interceptación del tráfico de red (Man-in-the-Middle). · Configuración incorrecta de routers, switches y firewalls. · Uso de protocolos inseguros o sin cifrado. · Uso de redes Wi-Fi inseguras. · Saturación del ancho de banda. · Puntos de acceso inalámbricos no autorizados (Rogue Access Point). · Falta de segmentación de la red. · Accesos no autorizados a la infraestructura de red. · Monitoreo insuficiente del tráfico de red.
Aplicaciones WEB	· Ataques por inyección SQL. · Cross-Site Scripting (XSS). · Cross-Site Request Forgery (CSRF) · Frameworks y bibliotecas desactualizadas. · Configuración insegura del servidor web. · Ausencia, vencimiento o configuración incorrecta de certificados SSL/TLS. · Exposición de endpoints o servicios REST. · Gestión inadecuada de sesiones y autenticación. · Divulgación de información sensible mediante mensajes de error. · Carga insegura de archivos (File Upload).
Infraestructura tecnológica	· Fallas en el suministro eléctrico. · Descargas eléctricas y variaciones de voltaje. · Incendios. · Inundaciones o filtraciones de agua. · Sismos u otros fenómenos naturales. · Fallas o ausencia de sistemas de climatización y refrigeración. · Deficiencias en el sistema de cableado estructurado. · Acceso físico no autorizado a las instalaciones. · Insuficiencia de vigilancia física y control de acceso. · Fallas en el centro de datos o cuarto de servidores. · Interrupciones en los servicios de telecomunicaciones. · Ausencia de sistemas de energía ininterrumpida (UPS) o plantas de emergencia.

Procedimientos	· Ausencia o deficiencia de canales de comunicación, difusión y distribución de la información. · Ausencia o deficiencia en la documentación estratégica: políticas de seguridad, manual de funciones, plan de administración del riesgo, plan de continuidad del negocio y plan de recuperación ante desastres. · Ausencia o deficiencia de procesos de auditoría informática y seguimiento de hallazgos. · Ausencia de procedimientos para la gestión de cambios en infraestructura, aplicaciones y bases de datos. · Ausencia de procedimientos para la administración de usuarios, privilegios y accesos. · Deficiencias en los procedimientos de respaldo, restauración y verificación de copias de seguridad. · Ausencia de procedimientos para la actualización y aplicación de parches de seguridad. · Falta de procedimientos para la clasificación y manejo de la información. · Deficiencias en el registro, conservación y revisión de bitácoras (logs) de seguridad. · Ausencia de procedimientos para la gestión de proveedores y terceros con acceso a información institucional. · Deficiencias en los procedimientos de respuesta, comunicación y escalamiento durante incidentes de ciberseguridad. · Ausencia de indicadores para evaluar la eficacia de los controles implementados. · Falta de revisión y actualización periódica de políticas, procedimientos y estándares institucionales.
Recursos humanos	· Falta de capacitación en ciberseguridad. · Desconocimiento de políticas y procedimientos institucionales. · Ingeniería social (phishing, vishing, smishing). · Uso de contraseñas débiles o reutilizadas. · Divulgación accidental de información confidencial. · Uso indebido de privilegios de acceso. · Incumplimiento de políticas de seguridad. · Acceso de exempleados por cuentas no deshabilitadas. · Amenazas internas (insider threats). · Resistencia al cumplimiento de controles y buenas prácticas de seguridad.
Recursos materiales	· Insuficiencia de presupuesto para ciberseguridad. · Obsolescencia del equipamiento tecnológico. · Falta de licenciamiento de software y herramientas de seguridad. · Deficiencia en la adquisición de equipos certificados. · Insuficiencia de dispositivos de respaldo y almacenamiento. · Carencia de sistemas de alimentación ininterrumpida (UPS). · Inventario desactualizado de activos tecnológicos. · Pérdida, robo o extravío de activos informáticos. · Mantenimiento insuficiente del equipamiento tecnológico. · Mobiliario inadecuado

Nota: Cada riesgo se puede desarrollar con la estructura del plan de administración de riesgo.

La diversidad de riesgos señalados en la matriz encuentra correspondencia con situaciones documentadas recientemente en instituciones públicas mexicanas. En diciembre de 2025, la Secretaría Anticorrupción y Buen Gobierno informó sobre incidente de seguridad relacionado con bases de datos personales de instituciones públicas, cuya investigación consideró el origen del incidente y posibles fallas en los controles de seguridad, credenciales y accesos. Asimismo, en septiembre de 2025, la Guardia Nacional recibió la Declaración de Cumplimiento del CERT-MX bajo el Modelo SIM3 CSIRTAmericas Baseline, orientado a evaluar la madurez y capacidades de los equipos de respuesta ante incidentes.

En conjunto, estos antecedentes refuerzan la pertinencia de valorar cada riesgo considerando el activo afectado, la vulnerabilidad, la amenaza, el impacto potencial y las medidas de tratamiento (Secretaría Anticorrupción y Buen Gobierno, 2025; Guardia Nacional, 2025).

ISO/IEC 27001 como modelo de gobernanza

La gobernanza de la ciberseguridad requiere un modelo que permita traducir las decisiones estratégicas de la organización en políticas, procedimientos, controles y mecanismos de evaluación permanentes. En este contexto, la norma ISO/IEC 27001 constituye uno de los principales referentes internacionales para implementar un SGSI, proporcionando un marco metodológico orientado a proteger la confidencialidad, integridad y disponibilidad de la información mediante un enfoque basado en riesgos y en la mejora continua (ISO/IEC_27001, 2022).

Para lograr este propósito, la norma establece dimensiones organizadas conforme al ciclo de mejora continua, que comprenden el contexto de la organización (4), el liderazgo (5), la planificación (6), el soporte (7), la operación (8), la evaluación del desempeño (9) y la mejora continua (10). Estas permiten que las organizaciones desarrollen un SGSI alineado con sus objetivos institucionales y con un enfoque permanente de gestión del riesgo (NQA, 2025).

Como apoyo a la implementación del sistema de gestión de seguridad de la información, se diseña el instrumento para el reporte integral del nivel de madurez en cumplimiento de la norma ISO27001, para definir los procesos de lo general a lo particular con activos de información y partes interesadas. (ISO_27001:27002). (ver tabla 12)

Tabla 12. Reporte integral en cumplimiento de la norma ISO27001.

Institución / Organización:	Folio: 1/N
Área o Proceso Auditado:	Fecha: / /
Responsable del Área:	Auditoría: Externa
Nivel de Cumplimiento Integral:	

Instrucción para la evaluación del nivel de madurez:

- El nivel de madurez de cada dimensión se obtiene a partir de la evaluación individual de sus componentes.
- Cada subcomponente, (4.1.1, 4.1.2 y 4.1.3) deberá calificarse conforme a la escala establecida. Posteriormente, se calculará el promedio de las calificaciones obtenidas para determinar el nivel de madurez del componente correspondiente (en este caso: 4.1).
- Finalmente, el nivel de madurez de la dimensión se obtendrá mediante el promedio de los componentes que la integran.

Organización y su contexto	Liderazgo	Planificación	Soporte	Operación	Evaluación desempeño	Mejora

Escala de evaluación del nivel de madurez

1. Inexistente: No existe evidencia de la implementación del requisito o control evaluado.
2. Básico: El requisito o control se aplica de manera parcial o informal; existen prácticas aisladas, pero no se encuentran documentadas ni estandarizadas.
3. Medible: El requisito o control se encuentra documentado, implementado y es evaluado periódicamente mediante evidencias objetivas que permiten verificar su cumplimiento.
4. Optimizado: El requisito o control se encuentra plenamente implementado, es monitoreado de forma continua, se evalúa su eficacia y se fortalece mediante acciones de mejora continua.

4	El contexto de la organización	Nivel
4.1	Entendiendo la organización y su contexto.	
4.1.1	¿Están identificados los objetivos del Sistema de Gestión de Seguridad de la Información (SGSI)?	
4.1.2	¿Se han identificado las cuestiones internas y externas relacionadas con la seguridad de la información?	
4.1.3	¿Se han identificado cómo las partes internas y externas pueden suponer amenazas o riesgos para la seguridad de la información?	
4.2	Expectativas de las partes interesadas.	
4.2.1	¿Se han identificado las partes interesadas?	
4.2.2	¿Existe un listado de requisitos sobre seguridad de la información de las partes interesadas?	
4.2.3	¿Existe un listado de requisitos sobre seguridad de la información referente a reglamentos, requisitos legales y requisitos contractuales?	
4.3	Alcance del SGSI.	
4.3.1	¿Se ha determinado el alcance del SGSI y se conserva información documentada?	
4.4	Sistema de Gestión de la Seguridad de la Información	
4.4.1.	¿El SGSI está establecido, implementado y se revisa de forma planificada considerando oportunidades de mejora?	
5	**Liderazgo**	**Nivel**
5.1	Liderazgo y compromiso.	
5.1.1	¿Se han establecido objetivos de la seguridad de la información acordes con los objetivos del negocio?	
5.1.2	¿La dirección provee los recursos materiales y humanos necesarios para el cumplimiento de los objetivos del SGSI?	
5.1.3	¿La dirección revisa la eficacia del SGSI para garantizar que se cumplen sus objetivos?	
5.2	Política de la seguridad de la información	
5.2.1	¿Se ha definido una Política de la Seguridad de la Información?	
5.2.2	¿Se ha establecido un marco que permita el establecimiento de objetivos?	
5.2.3	¿Se difunde la política de la seguridad de la información a las partes interesadas?	
4.2.4	¿Se mantiene información documentada de la política del SGSI y de sus objetivos?	
5.3	Roles y responsabilidades.	

5.3.1	¿Se han asignado las responsabilidades y autoridades sobre la seguridad de la información?	
5.3.2	¿Se han comunicado las responsabilidades y autoridades para la seguridad de la información?	
6	**Planificación**	**Nivel**
6.1	Tratamiento de riesgos y oportunidades.	
6.1.1	¿El plan para abordar riesgos y oportunidades considera las expectativas de las partes interesadas en relación con la seguridad de la información?	
6.1.2	¿Se identifican y analizan los riesgos mediante un método de evaluación y aceptación de riesgos?	
6.1.3	¿Se ha definido un proceso de tratamiento de riesgos?	
6.1.4	¿Se han establecido criterios para elaborar una declaración de aplicabilidad?	
6.1.5	¿Se mantiene información documentada de los puntos anteriores?	
6.2	Planificación para consecución de objetivos.	
6.2.1	¿Se han establecido objetivos de la seguridad de la información medibles y acordes a los objetivos del negocio?	
6.2.2	¿Los objetivos de la seguridad de la información están planificados mediante: -asignación de responsabilidades; -cronograma de ejecución temporal; -método de evaluación?	
6.2.3	¿Se han integrado los objetivos de la seguridad de la información en los procesos de la organización teniendo en cuenta las funciones principales dentro de esta?	
7	Soporte	
7.1	Recursos.	
7.1.1	¿Se identifican y asignan los recursos necesarios para el SGSI?	
7.2	Competencia.	
7.2.1	¿Se evalúa la competencia en materia de seguridad de la información para personas que efectúan tareas que puedan afectarla?	
7.2.2	¿Se mantiene información actualizada sobre la competencia del personal?	
7.3	Concienciación.	
7.3.1	¿El personal está involucrado y es consciente de su papel en la seguridad de la información?	
7.3.2	¿Existe consciencia de los daños que se pueden producir de no seguir las pautas de la seguridad de la información?	

7.4	Comunicación.	
7.4.1	¿Se comunica la política de la seguridad de la información con las responsabilidades de cada uno?	
7.4.2	¿Existe un proceso para comunicar las deficiencias o malas prácticas en la seguridad de la información?	
7.5	Información documentada.	
7.5.1	¿Existe documentación requerida por la norma más la requerida por la organización incluyendo: – la política de la seguridad de la información y el alcance del Sistema de Gestión; – los procesos principales de la seguridad de la información; – los documentos exigidos por la Norma ISO 27001 incluyendo registros; – los documentos propios de seguridad de la información identificados por la empresa (instrucciones técnicas, etc.)?	
7.5.2	¿Existe un control documental donde se verifica: -quién publica el documento; -quién lo autoriza y cómo se revisa; -formatos y soportes de publicación; -su almacenamiento y protección?	
7.5.3	¿Se controlan los documentos de origen externo?	
8	**Operación**	**Nivel**
8.1	Control operacional.	
8.1.1	¿Los procesos de seguridad de la información están documentados para controlar que se realizan según lo planificado?	
8.1.2	¿Existe un proceso para evaluar los riesgos en la seguridad de la información antes de realizar cambios en el Sistema de Gestión o procesos de seguridad?	
8.1.3	¿Se establecen medidas y planes para mitigar los riesgos en la seguridad de la información ante cambios realizados?	
8.1.4	¿Se identifican y controlan los procesos externalizados en cuanto a los riesgos para la seguridad de la información?	
8.2.	Análisis de riesgos de la seguridad de la información.	
	¿Se ha establecido un proceso documentado de análisis y evaluación de riesgos para la seguridad de la información donde se identifique: -el propietario del riesgo; -la importancia del riesgo o nivel de impacto; -la probabilidad de ocurrencia?	
8.3	Tratamiento de riesgos de la seguridad de la información.	
8.3.1	¿Se ha implementado un plan de tratamiento de riesgos dónde: -los propietarios del riesgo están informados y han aprobado el plan; -se documentan los resultados?	

8.3.2	¿Se identifican todos los controles necesarios para mitigar el riesgo justificando su aplicación?	
8.3.3	¿Se documenta el nivel de aplicación de todos los controles a aplicar?	
9	**Evaluación del desempeño**	**Nivel**
9.1	Seguimiento y medición.	
9.1.1	¿Existe un proceso continuo de monitoreo de la seguridad de la información teniendo en cuenta los controles?	
9.1.2	¿Existe un proceso documentado para evaluar los resultados de las mediciones y que estos sean tomados en cuenta por los responsables de la seguridad de la información?	
9.2	Auditorías internas.	
9.2.1	¿Se ha establecido una programación de auditorías internas y asignado responsables?	
9.2.2	¿Se ha definido el alcance y los requisitos para el informe de auditoría?	
9.2.3	¿Se consideran acciones correctivas y propuestas de cambio en los informes de auditoría?	
9.3	Informe de revisión por la dirección.	
9.3.1	¿Existe una programación para los informes de la dirección y constancia de realización periódica?	
9.3.2	¿Se documentan los resultados de los informes y la dirección implica su conocimiento en la toma de decisiones sobre los aspectos cruciales para el SGSI?	
10	**Mejora continua**	**Nivel**
10.1	No conformidades y acciones correctivas.	
10.1.1	¿Existe un procedimiento documentado para registrar las no conformidades y su tratamiento?	
10.1.2	¿Dentro de las acciones correctivas existe una diferenciación entre acciones correctivas sobre la no conformidad y sobre las causas de la misma?	
10.2	Mejora continua.	
10.2.1	¿Existe un proceso para garantizar la mejora continua del SGSI identificando las oportunidades?	
	Revisión del análisis Auditor _____	

Nota: El instrumento fue desarrollado con fundamento en ISO_27001:27002.

Y con el propósito de obtener una evaluación sistemática de criterios, mediante el desarrollo de preguntas que denotan hallazgos, evidencias, recomendaciones y riesgos, y facilitar su aplicación práctica y réplica en organizaciones públicas y privadas; se diseñan los instrumentos específicos por dimensión; en donde, los hallazgos se clasifiquen en Conformidad (C), Conformidad Condicionada (CC) y No Conformidad (NC), de acuerdo con el grado de cumplimiento de los requisitos evaluados.

Como aportación de valor se presenta el instrumento para la dimensión 4., en el *Anexo 3. La organización y su contexto.*

Con un enfoque más técnico, se encuentra la ISO/IEC 27002 que orienta la selección e implementación de los controles necesarios para el tratamiento de los riesgos identificados.

Entre sus principales dominios se encuentran

- Políticas de seguridad de la información
- Organización de la seguridad de la información
- Seguridad relativa a los recursos
- Gestión de activos
- Control de acceso
- Criptografía
- Seguridad física y del entorno
- Seguridad de las operaciones
- Seguridad en las comunicaciones
- Adquisición, desarrollo y mantenimiento de los sistemas de información
- Relación con proveedores
- Gestión de incidentes de la seguridad de la información
- Aspectos de seguridad de la información en la gestión de continuidad del negocio
- Cumplimiento

La aplicación sistemática de estos controles permite fortalecer la gobernanza de la ciberseguridad al integrar medidas preventivas, detectivas y correctivas dentro de los procesos organizacionales.

Capítulo II.

Seguridad Técnica e Infraestructura Digital

Introducción

La ciberseguridad organizacional se encuentra influenciada tanto por las capacidades internas como por las presiones provenientes del entorno, especialmente aquellas derivadas de las cadenas de suministro y de los organismos reguladores (Arroyabe, MF. et al, 2026). Las redes de comunicación, servicios en la nube, dispositivos inteligentes, plataformas digitales e infraestructuras críticas conforman un ecosistema cuya operación depende de la disponibilidad, integridad y confidencialidad de la información. En consecuencia, la seguridad técnica constituye un elemento esencial para garantizar la continuidad de las operaciones y la protección de los activos digitales.

La evolución de las amenazas ha demostrado que la incorporación de tecnologías emergentes, incluida la inteligencia artificial, también ha sido aprovechada por la ciberdelincuencia para desarrollar ataques más sofisticados, automatizados y difíciles de detectar. Como señalan Salem et al. (2024), el incremento tan-to en el número como en la complejidad de los ciberataques ha hecho indispensable fortalecer los mecanismos de detección y

respuesta mediante técnicas avanzadas de ciberseguridad. Por ello, resulta necesario adoptar arquitecturas de seguridad, mecanismos de autenticación, estrategias de protección de redes, análisis de vulnerabilidades y capacidades de respuesta que permitan fortalecer la resiliencia tecnológica de las organizaciones.

Este capítulo desarrolla los fundamentos técnicos de la ciberseguridad, abordando los controles, que permiten proteger la infraestructura digital frente a un entorno de amenazas en constante evolución. Abordando la importancia de la seguridad de las bases de datos, priorizando la adopción de buenas prácticas, detección de vulnerabilidades, reconocimiento de ataques y medidas de prevención. Así también, se incluye buenas prácticas en plataformas digitales y dispositivos móviles.

Como propuesta de valor se comparte las principales medidas para la mitigación del riesgo.

Seguridad de bases de datos

La seguridad de bases de datos comprende el conjunto de controles técnicos, administrativos y operativos orientados a preservar la confidencialidad, integridad y disponibilidad de la información almacenada, mediante mecanismos que previenen el acceso no autorizado, la alteración, la pérdida o la divulgación indebida de los datos. En la actualidad, la protección de las bases de datos representa uno de los mayores desafíos para los gestores, debido a la creciente sofisticación de los ataques informáticos y a la necesidad de implementar medidas de seguridad durante todo el ciclo de vida del desarrollo de software, desde el diseño hasta la operación y mantenimiento de los sistemas (Iqbal & et al., 2023).

Las bases de datos constituyen uno de los activos más valiosos de la organización, debido a que almacenan de forma sistematizada información personal, financiera, administrativa y estratégica, alojada en servidores locales o servicios en la nube. En consecuencia, su seguridad debe abordarse desde una perspectiva integral que considere tanto la infraestructura tecnológica como

las aplicaciones que interactúan con ellas, incorporando mecanismos de autenticación, autorización, control de acceso, cifrado, privacidad de los datos y estrategias de mitigación de riesgos.

Diversas investigaciones reconocen que las principales amenazas para la seguridad de las bases de datos se relacionan con sistemas de autorización deficientes, controles de acceso débiles, fugas de información, vulnerabilidades en las aplicaciones y ataques dirigidos a las bases de datos, lo que obliga a las organizaciones a fortalecer continuamente sus controles preventivos y correctivos (Iqbal & et al., 2023).

Asimismo, la protección de las bases de datos no solo responde a necesidades técnicas, sino también al cumplimiento de las obligaciones jurídicas previstas en el marco normativo mexicano en materia de protección de datos personales, transparencia y acceso a la información pública, contribuyendo a la protección de los datos personales, al respeto de los derechos fundamentales y garantizando la continuidad de las operaciones.

Buenas prácticas con bases de datos

Bajo este enfoque, los administradores y desarrolladores de tecnología deben garantizar la seguridad de las bases de datos tanto a nivel físico como lógico. El primero se orienta a la protección de la infraestructura y los componentes de hardware, como ordenadores, discos duros externos, servidores y demás dispositivos, así como de las instalaciones y áreas destinadas a su operación, con el propósito de asegurar su funcionamiento óptimo y confiable. El segundo comprende la protección del software de sistema y de aplicación, dentro del cual el sistema de gestión de bases de datos (SGBD) constituye uno de los principales componentes susceptibles de presentar vulnerabilidades y ser objeto de accesos no autorizados.

En este sentido, la protección lógica de las bases de datos requiere la implementación de controles orientados a restringir

el acceso, preservar la confidencialidad e integridad de la información y reducir la posibilidad de uso indebido. Entre los principales controles se encuentran:

- Como primer elemento de defensa, se define el control de acceso, por medio de cuentas de usuario y contraseñas,
- A partir de lo anterior, se puede implementar la clasificación de datos y usuarios con una restricción de [Información Confidencial], permitiendo el acceso a usuarios autorizados por definición o revocación de privilegios, o por asignación de niveles de seguridad, lo que puede variar según el grado de confidencialidad.
- Incorporar una especialización que active algunos usuarios o grupos de usuarios a segmentos específicos (entidades, registros y campos).
- Controlar la acción de lectura, escritura y actualización de datos por administración de usuarios.
- Cifrar datos.
- Implementar mecanismos de autenticación multifactor para las cuentas administrativas y privilegiadas.
- Mantener actualizado el Sistema Gestor de Bases de Datos mediante la instalación de parches y actualizaciones de seguridad proporcionadas por el fabricante.
- Mantener habilitados los registros de auditoría (logs) para identificar accesos, modificaciones, consultas y demás actividades relevantes sobre la base de datos.

Sin embargo, la base de datos es un activo codiciable en riesgo permanente, que exige medidas de seguridad acordes a la innovación tecnológica, por la obligación de salvaguardar los datos personales e información sensible:

- Implementar una política de respaldo mediante copias de seguridad periódicas en medios locales, extraíbles, virtuales o en la nube, para salvaguardar la información ante filtraciones, fallos del sistema, eliminación accidental de datos u otras eventualidades técnicas.
- Plan de contingencia y protocolos de recuperación.
- Protocolo para la administración de archivos, ficheros y bitácoras del sistema, que permita mantener un registro detallado de accesos, modificaciones, incidencias e intervenciones realizadas sobre la base de datos.
- Aplicar el principio de mínimo privilegio, otorgando únicamente los permisos indispensables para el desempeño de las funciones asignadas.
- Revisar periódicamente las cuentas de usuario para deshabilitar o eliminar aquellas que ya no se utilicen.
- Separar los ambientes de desarrollo, pruebas y producción, evitando utilizar información real fuera del entorno autorizado.
- Verificar periódicamente la integridad de las copias de seguridad mediante pruebas de restauración, con la finalidad de garantizar la recuperación efectiva de la información.

Vulnerabilidades en bases de datos

Las bases de datos pueden verse comprometidas por errores de configuración de protocolos, fallas en el desarrollo de aplicaciones, autenticación con contraseñas débiles parches desactualizados, exposición de respaldo en sitios vulnerables, cifrado deficiente o inexistente, servicios abiertos a internet, errores en la configuración de roles, asignación de privilegios excesivos y técnicas de ataque entre las cuales destaca la inyección SQL (Structured Query Language). Las vulnerabilidades se pueden presentar, cuando:

- Existen errores en la configuración del Sistema Gestor de Bases de Datos que definen incorrectamente los parámetros y habilitan servicios innecesarios.
- Las cuentas tienen contraseñas débiles, compartidas o predeterminadas por el sistema.
- Se mantienen cuentas de usuarios inactivas o credenciales de exempleados que conservan privilegios sobre la base de datos.
- Se asignan privilegios superiores a los necesarios por rol de usuario, permitiendo el acceso a servicios o procedimientos con información sensible.
- No se ejecutan en forma y tiempo las actualizaciones al Sistema Gestor de Bases de Datos, otorgada por el desarrollador o el sistema, generando un espacio de incertidumbre para la explotación de una vulnerabilidad.
- Las copias de respaldo o de seguridad se encuentran expuestas sin mecanismos de control de acceso o de cifrado; o en su defecto, son de bajo nivel de cobertura.
- La publicación de servicios de bases de datos en internet no cuenta con una segmentación de red y controles de autenticación eficientes.

Actualmente, la gestión de vulnerabilidades requiere superar su identificación y considerar su relevancia para determinar cuáles deben atenderse con mayor prioridad. En 2026, el NIST-b adoptó para la *National Vulnerability Database* (NVD) un enfoque de priorización basado en riesgo, dando especial atención a las vulnerabilidades que cuentan con evidencia de haber sido explotadas en ataques reales. Entre ellas se encuentran CVE-2024-36401, que permitió la ejecución remota de código en GeoServer; CVE-2019-19781, asociada con la ejecución remota de código en Citrix ADC y Citrix Gateway; y CVE-2021-26855, utilizada para comprometer servidores Microsoft Exchange y acceder a información de los buzones de correo. Estos casos muestran que la existencia de una vulnerabilidad adquiere especial relevancia cuando puede ser explotada en condiciones reales.

En este contexto, la vulnerabilidad CVE-2021-20016 de SonicWall SMA 100 Series constituye un ejemplo de inyección SQL, en la que una entrada manipulada puede alterar la consulta enviada al sistema y permitir el acceso no autorizado a información o credenciales. Este tipo de vulnerabilidad evidencia la importancia de fortalecer la validación de entradas, los mecanismos de autenticación y los controles de acceso en los sistemas de bases de datos.

Como lo indica Mozilla en su portal: "La inyección SQL aprovecha las vulnerabilidades de las aplicaciones web que no validan la entrada del usuario" (MDN, s.f.). Este tipo de ataque compromete los ficheros de autenticación y se posiciona como la amenaza más crítica dentro de las aplicaciones WEB, exponiendo a la base de datos a las siguientes vulnerabilidades:

- Acceso no autentificado ni autorizado de usuarios a información confidencial como: cuentas de usuario, contraseñas, datos personales, financieros, organizacionales, etc.,
- Pérdida de integridad (destrucción o alteración) de la información, activando el riesgo financiero y reputacional, con efectos civiles y legales.
- Ejecución de sentencias y comandos, afectando directamente el procesamiento de las transacciones y el control de concurrencia intercalada.

Los tipos de ataques con inyecciones SQL son técnicas para manipular consultas y obtener o modificar datos sin autorización que se presentan de diferentes formas, cada uno con su propio método e impacto. Para poder prevenirlas primero es necesario identificarlas como lo señalan Conrad, 2024, y Sing y Yesil, 2026, en blogs, con ejemplos aplicativos.

- Inyección SQL en banda:

  Se produce cuando se envían consultas SQL maliciosas a través de la interfaz de la aplicación web.

- Ejemplo: Al introducir OR '1'='1', la instrucción es siempre verdadera y concede el acceso sin comprobar la contraseña.

- Inyección SQL basada en error:

  Se produce cuando la aplicación no devuelve el resultado de la consulta SQL, pero presenta un mensaje de error, que revela información confidencial sobre la base de datos. El éxito se determina analizando la respuesta y el comportamiento de la aplicación.

  - Ejemplo: Al introducir 1' OR '1'='1 siempre se evalua-rá como verdadera la igualdad, lo que podría revelar como mensajes de error los nombres de columnas o tablas en la base de datos.

- Inyección SQL basada en UNION:

  Se produce cuando la consulta usa el operador UNION para ejecutar otra consulta al mismo tiempo y extraer datos de otras tablas de la base de datos. Esta técnica deja expuesta la necesidad de validar las entradas y realizar una parametrización de consultas como mecanismo de prevención; similar a la anterior, se presentan mensajes de error que servirán de insumos para las consultas posteriores. Entre los comandos que potencializan los resultados se encuentran @@version y @current_user, para facilitar la versión de la base de datos y los privilegios del usuario.

- Inyección SQL ciega basada en booleanos:

  Requiere un método de prevención específico cuando la consulta obliga a la base de datos a devolver un resultado booleano verdadero si la condición se cumple, y falso en caso contrario. Es decir, proporciona dos estados: información del registro o registro no encontrado.

- Inyección SQL ciega basada en el tiempo:

  Esta opción presenta sus propios desafíos en relación con el tiempo de respuesta del servidor. Cuando se ejecuta una consulta con la condición (1=1) se evalúa la condición; si es verdadera, la base de datos se detendrá 5 segundos; de lo contrario, la sentencia será nula. De esta forma se va midiendo la estructura y para comprobar la inyección se emplea la función *sleep,* como se presenta a continuación:

  *Select * from users where username = 'admin' and if(1=1, sleep(5), null) and '1'='1' and password = 'password';*

El Cross-Site Scripting (XSS) es una vulnerabilidad que permite al atacante inyectar un código malicioso en una página web, que ocurre cuando se incluyen datos no confiables en la salida HTML, sin una validación previa y codificación adecuada; esto confunde al navegador y ejecuta el script inyectado como legítimo. La secuencia de comandos entre sitios Cross-Site Scripting (XSS) se clasifica en tres tipos, según Invicti, 2026.

- Reflejada (Reflected): Entre sitios no persistentes; en don-de, el código malicioso se inserta en una solicitud HTTP y se refleja en la respuesta del servidor, lo que afecta únicamente a los usuarios que ingresan al enlace malicioso.
- Almacenada (Stored): Entre sitios almacenados o persistentes, donde el código inyectado se almacena permanentemente en el servidor, afectando a todos los usuarios que acceden al contenido comprometido.
- Basada en el DOM (DOM-based): Manipula el modelo de objetos del documento del navegador del usuario para ejecutar scripts no autorizados.

La gestión de vulnerabilidades incorpora también automatización e inteligencia artificial para procesar y analizar grandes

volúmenes de información. En 2026, el NIST modernizó la NVD con nuevos elementos de evaluación y priorización, reforzando la valoración de las vulnerabilidades según su contexto, exposición e impacto (NIST-c, 2026).

Técnicas de ataque y reconocimiento

- Antes de comprometer un sistema, el atacante realiza actividades de reconocimiento con la finalidad de identificar los servicios disponibles, los puertos abiertos, los protocolos empleados y las posibles vulnerabilidades del entorno tecnológico. Entre las estrategias más recurrentes para dirigir un ataque, se identifican las siguientes:
- Envío de mensajes fraudulentos que confunden al administrador y otorga consensualmente el acceso a la base de datos.
- Pesca de cookies (programas que almacenan los datos de la navegación en internet) para obtener las credenciales de los usuarios.
- Peticiones recurrentes, enviadas al servidor con la finalidad de medir su seguridad.

Estas prácticas corresponden a la fase de reconocimien-to del ataque, cuyo propósito consiste en obtener información suficiente sobre la infraestructura tecnológica para seleccionar la técnica de explotación con mayores probabilidades de éxito. Ante la premisa de anular o minimizar los intentos de intrusión mediante inyecciones SQL, se comparten los siguientes procedimientos:

- Escaneo de la red mediante herramientas como Nmap para identificar hosts activos, puertos abiertos, servicios publicados, versiones de software y sistemas operativos utilizados por los dispositivos conectados.

- Enumeración de servicios y versiones para identificar software obsoleto, configuraciones inseguras y vulnerabilidades conocidas susceptibles de explotación, reduciendo la superficie de ataque mediante la desactivación de servicios que no participan en la operación normal del sistema.
- Obtención de banners de los servicios publicados (Banner Grabbing), con el propósito de identificar versiones de servidores web, bases de datos y aplicaciones expuestas, facilitando su comparación con vulnerabilidades conocidas.
- Monitoreo del tráfico de red mediante Wireshark para analizar las tramas intercambiadas entre clientes y servidores, identificar protocolos utilizados, detectar comportamientos anómalos y reconocer posibles vulnerabilidades durante la comunicación.

El análisis del tráfico de red permite identificar patrones normales y anómalos de comunicación, facilitando la detección temprana de actividades de reconocimiento, exploración de servicios, conexiones no autorizadas o incrementos inusuales del tráfico.

Durante el monitoreo del tráfico resulta conveniente analizar los protocolos y puertos utilizados por los servicios de red. Por ejemplo:

- TCP 80 (HTTP), para identificar comunicaciones sin cifrado.
- TCP 443 (HTTPS), para verificar el uso de conexiones seguras.
- UDP 53 (DNS), cuyo incremento inusual de consultas puede evidenciar intentos de resolución de dominios maliciosos.
- TCP 21 (FTP) y TCP 23 (Telnet), cuya utilización representa un riesgo al tratarse de protocolos inseguros que pueden sustituirse por alternativas más robustas como SFTP o SSH.

- Escaneo automatizado de vulnerabilidades mediante herramientas especializadas para identificar configuraciones inseguras, software desactualizado y debilidades conocidas antes de que puedan ser aprovechadas por un atacante.
- Búsqueda avanzada en Google para el reconocimiento de parámetros sensibles o errores de configuración sobre páginas web, con la técnica Google Dorking, que permite localizar directorios, archivos de respaldo, paneles de administración, mensajes de error y otros recursos publicados de forma involuntaria por configuraciones inseguras.
- Identificación de servicios innecesarios habilitados en servidores y dispositivos de red, reduciendo la superficie de ataque mediante la desactivación de aquellos que no participan en la operación normal del sistema.
- Identificación de las reglas de seguridad para filtrar el tráfico HTTP no deseado o malicioso en el sitio web y permitir solo el tráfico seguro, denegando el acceso mediante firewalls de aplicaciones web (Web Application Firewall, WAF), con el propósito de prevenir, detectar y bloquear solicitudes maliciosas antes de que alcancen la aplicación o la base de datos; mediante:

    - Amenazas de internet, incluidas direcciones de protocolo de internet (Internet Protocol, IP), encabezados de protocolo de transferencia de hipertexto (hypertext transfer protocol, HTTP), cuerpo HTTP, cadenas de identificador uniforme de recursos (uniform resource identifier, URI).
    - Ataques a las aplicaciones web; entre los que se destacan:
        - Inyección SQL (SQL Injection), mediante consultas maliciosas dirigidas a vulnerar la base de datos.
        - Scripts de sitios cruzados (Cross-Site Scripting, XSS): el usuario accede a scripts maliciosos de forma incauta durante la sesión de navegación.

- Falsificación de petición de sitios cruzados (Cross-Site Request Forgery, CSRF): el usuario autenticado es inducido a ejecutar acciones no deseadas dentro de la aplicación web. Como medidas preventivas se recomienda incorporar:
  - Tokens anti CSRF que sean validados por el servidor antes de procesar la petición.
  - Validación de origen y referente a peticiones para realizar la asociación con la aplicación.
  - Configurar el atributo "samesite" en las cookies de sesión.

- Denegación de servicio centralizado o distribuido (DoS/DDoS); que provoca la indisponibilidad de los servicios mediante la saturación del tráfico ocasionado por el atacante.
- Intercepción de comunicaciones Man-in-the-Middle (MitM); el atacante intercepta la comunicación entre dos sistemas para capturar, modificar o redirigir la información intercambiada, comprometiendo credenciales, sesiones y transacciones. Como medidas de prevención se recomienda:
  - Utilizar protocolos cifrados como HTTPS, TLS y VPN.
  - Implementar autenticación robusta y certificados digitales válidos.
  - Segmentar la red mediante VLAN y listas de control de acceso (ACL).
  - Mantener actualizados los sistemas operativos, dispositivos de red y firmware.

Como medidas de detección se recomienda:

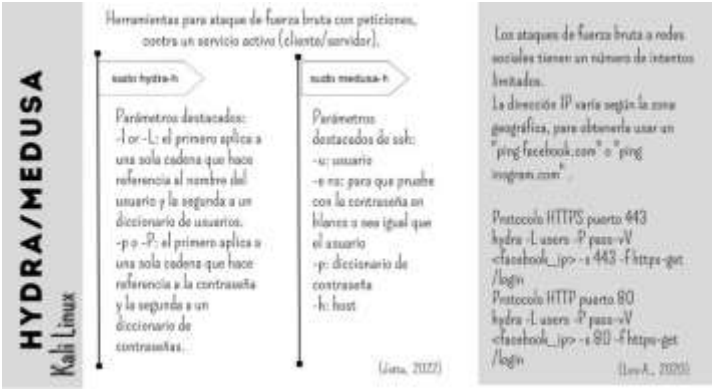
- Monitorear el tráfico mediante herramientas como Wireshark o sistemas IDS/IPS.
- Analizar respuestas ARP, consultas DNS y conexiones no cifradas.

Como medidas de corrección:

- Aislar el dispositivo comprometido.
- Restablecer certificados y credenciales.
- Revisar la configuración de la infraestructura y aplicar los parches correspondientes.

o Ataque de fuerza bruta mediante herramientas como Hydra o Medusa, utilizadas para evaluar la robustez de las credenciales y los mecanismos de autenticación multifactor (MFA), hasta lograr el acceso mediante múltiples combinaciones de usuario y contraseña (ver figura 10).

Figura 10. Hydra.



Para reducir este riesgo se recomienda:

- Limitar el número de intentos de autenticación.
- Registrar y monitorear los eventos de autenticación mediante bitácoras (logs).
- Bloquear temporalmente las cuentas o direcciones IP después de múltiples intentos fallidos.

- Pruebas de inyección SQL, con SQL Map, que identifican y explotan vulnerabilidades en aplicaciones web conectadas a las bases de datos.
- Pruebas de penetración en entornos controlados mediante aplicaciones deliberadamente vulnerables como Damn Vulnerable Web Application (DVWA), utilizadas con fines académicos y de evaluación para fortalecer los mecanismos de defensa antes de la puesta en producción de los sistemas.

Además de los Web Application Firewall (WAF), las organizaciones implementan firewalls de red para controlar el tráfico entre segmentos de la infraestructura, firewalls de host para proteger equipos individuales y, cada vez con mayor frecuencia, firewalls de nueva generación (NGFW), capaces de inspeccionar aplicaciones, usuarios y contenido, integrando funciones de prevención de intrusiones y análisis de amenazas. Para las bases de datos desarrolladas con lenguajes alternos, también existen herramientas NoSQL, que emplean una dinámica diferente, pero tienen el mismo propósito: identificar vulnerabilidades antes de que puedan ser explotadas.

Es por ello que la mejor forma para lidiar con un ataque a la base de datos es no esperar que suceda, sino realizar pruebas o testeos continuos para detectar las consultas que vulneran al servidor, antes de que las vulnerabilidades sean explotadas. La supervisión permanente de la infraestructura tecnológica fortalece la disponibilidad de los servicios, protege la información, reduce la probabilidad de incidentes de seguridad y contribuye con el cumplimiento de las obligaciones de protección de la información. De esta manera se puede tomar medidas preventivas sobre:

- La configuración de los permisos de usuarios a tablas y de privilegios de lectura y escritura a registros.
- La penalización de algunas palabras clave, aunque no es una práctica muy recomendable.

- Protección del diccionario del servicio SSH (Secure Shell) evitando configuraciones predeterminadas que relacionan el protocolo al puerto número 22 y limitar los intentos de acceso a nivel usuario, con lo que se fortalecen los mecanismos de acceso.

Finalmente, las actividades de reconocimiento no deben considerarse exclusivas de los atacantes. También constituyen una práctica preventiva para administradores, auditores y responsables de seguridad, quienes, mediante el monitoreo permanente, el análisis del tráfico y las pruebas de evaluación pueden identificar oportunamente vulnerabilidades, reducir la superficie de ataque y fortalecer la confidencialidad, integridad, disponibilidad y continuidad operativa de los servicios tecnológicos.

Controles de protección para aplicaciones web

Las contraseñas de los sitios o páginas web también se encuentran en riesgo sino existe una conexión segura a internet con datos autenticados y encriptados entre el servidor y cliente; entre las medidas de prevención se encuentra la adopción del protocolo HTTPS (Hyper Text Transfer Protocol Secure) y el certificado de seguridad que aparece en la barra de direcciones, por las características que a continuación se detallan:

- El protocolo HTTP (Hypertext Transfer Protocol) permite la transferencia de la información entre el navegador y el servidor; sin embargo, para fortalecer las páginas o servicios se debe emplear su predecesor HTTPS, que incluye en la actualización el certificado digital de seguridad.
- El certificado digital emplea el protocolo TLS (Transport Layer Security) para establecer una comunicación confidencial entre el cliente y el servidor mediante algoritmos criptográficos, cifrado simétrico y funciones hash (ver figura 11). El proceso consiste en calcular, cifrar y descifrar la clave de sesión utilizando la clave pública contenida

en el certificado digital y la clave privada del servidor, permitiendo generar una clave maestra compartida para interpretar correctamente los mensajes intercambiados (Caballero Velasco & Cilleros Serrano, 2022).

Figura 11. Certificado SSL.



El protocolo genera confiabilidad, pero encuentra su talón de Aquiles en el momento de la renegociación del tipo de cifrado, quedando expuesto ante una posible inyección de código malicioso; por ello se sugiere mantener las versiones de SSL o TLS actualizadas, deshabilitar protocolos inseguros y verificar periódicamente la configuración de los certificados digitales.

Es importante señalar que la presencia del protocolo HTTPS y del certificado digital no garantizan, por sí mismos, que un sitio web sea legítimo o seguro; únicamente aseguran que la comunicación entre el cliente y el servidor se encuentra cifrada.

Cuando el navegador muestra advertencias como “Conexión no segura”, significa que el sitio web presenta problemas en la implementación del certificado digital SSL/TLS o utiliza una conexión que no garantiza la confidencialidad de la información transmitida. Esta situación puede deberse a certificados vencidos, configuraciones incorrectas o la ausencia del protocolo HTTPS. Ante una advertencia de conexión no segura se recomienda:

- No ingresar nombres de usuario, contraseñas, datos personales o información financiera.
- Verificar que exista una versión oficial del sitio utilizando HTTPS.
- Posponer el trámite cuando sea posible o utilizar un canal alterno oficial.
- Reportar la incidencia al administrador del portal cuando se trate de sitios institucionales.

En los casos que se requiera una autoexploración de las vulnerabilidades, se pueden emplear las herramientas *mitmproxy* y *sslstrip,* entre otras, en entornos autorizados y con fines de auditoría. Además, se pueden adoptar las recomendaciones siguientes:

- Verificar que el certificado digital corresponda realmente al dominio visitado, revisando la información del emisor, el periodo de vigencia y el nombre del sitio antes de proporcionar credenciales o información sensible.
- Implementar la Autenticación Multifactor (MFA) en aplicaciones web que administren información personal, financiera o institucional, disminuyendo el riesgo de acceso no autorizado cuando las credenciales sean comprometidas.
- Mantener actualizados los componentes de la aplicación web, incluyendo servidores, frameworks, bibliotecas, complementos y dependencias de software, con el propósito de corregir vulnerabilidades conocidas mediante la aplicación de parches de seguridad.
- Validar todas las entradas de datos recibidas desde formularios web para prevenir ataques por inyección SQL, ejecución de código y otras técnicas de explotación derivadas de entradas no controladas.
- Implementar políticas seguras para la administración de sesiones, evitar sesiones permanentes, establecer tiempos de expiración y eliminar automáticamente las sesiones inactivas.

Las contraseñas también se encuentran en riesgo cuando la conexión por internet se realiza mediante una red WiFi pública, aumentando la frecuencia de robo de datos por espionaje usando programas *sniffers* capaces de interceptar comunicaciones entre el usuario y los servicios web utilizados; mediante la vigilancia del tráfico de la red en tiempo real y capturas de tramas con información del usuario; indistintamente de la aplicación, plataforma web, sistema operativo, dispositivo móvil o computadora en uso.

La red pública brinda el derecho de internet gratuito para todos, pero no regula la conducta ni protege la privacidad de los internautas; es por ello que para minimizar el grado de vulnerabilidad se sugiere:

- No usar aplicaciones de mensajería instantánea, redes sociales ni correo electrónico para transmitir información sensible.
- No realizar transacciones financieras, como transferencias bancarias, pagos electrónicos y comercio electrónico.
- No ingresar credenciales de acceso a plataformas institucionales, servicios gubernamentales o aplicaciones corporativas.
- Evitar conectarse automáticamente a redes WiFi abiertas previamente utilizadas.
- Confirmar con el establecimiento el nombre oficial de la red inalámbrica antes de conectarse, evitando redes falsas creadas para suplantar puntos de acceso legítimos.
- Proteger las comunicaciones mediante el cifrado del envío y recepción de datos de extremo a extremo.
- Mantener una conexión de Red Privada Virtual (VPN) entre una comunidad de usuarios, contratada por su proveedor confiable.
- Desactivar la conexión automática al WiFi y al Bluetooth cuando no sean necesarios, reduciendo la posibilidad de conexiones no autorizadas.

- Verificar que las páginas web utilicen HTTPS antes de ingresar usuarios, contraseñas o información financiera, aun cuando se navegue mediante una VPN.

Aunque la contraseña cumpla con todas las medidas de prevención, se recomienda fortalecerla con la actualización periódica de todas las aplicaciones, sitios, páginas y dispositivos.

Los navegadores modernos incorporan mecanismos adicionales para fortalecer la protección durante la navegación, por lo que resulta recomendable mantener activadas sus funciones de seguridad. En específico para Google Chrome se recomienda verificar:

- Actualización del navegador.
- Contraseñas comprometidas o vulneradas.
- Navegación segura.
- Conexiones seguras.
- DNS seguro.

Buenas prácticas para plataformas digitales

Mensajería instantánea

Es un canal de comunicación bidireccional que permite el envío y recepción de contenido en formato de audio, video, imágenes y texto, mediante aplicaciones digitales como WhatsApp, Messenger, Telegram y similares.

Ante la amenaza constante de filtración a la cuenta y robo de información en estas aplicaciones, se sugieren las siguientes recomendaciones para brindar privacidad a la cuenta y fortalecer el grado de protección de los datos (ver figura 12):

Figura 12. Privacidad de la cuenta.

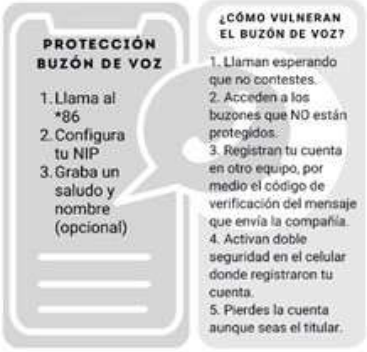


- Evitar envíos de datos personales, financieros, fiscales u otros, que pongan en riesgo la privacidad de la información, tales como INE, constancia del SAT, recibos de servicios básicos, estados de cuenta, tarjetas bancarias, recibos de nómina y otros.
- No ingresar a enlaces ni abrir archivos que induzcan a la sospecha de tener contenido malicioso.
- Vaciar y eliminar constantemente los grupos y chats innecesarios, que además de brindar una protección favorece el rendimiento del sistema.
- Respaldar en la computadora los documentos, fotografías, videos y audios.
- Eliminar fotografías *innecesarias* de la Galería y de la Carpeta de recuperación que las reserva por 30 días.
- Encriptar los datos sensibles enviados por mensajería instantánea, mediante:
    - Establecimiento de contraseñas de apertura, lectura y/o escritura de documentos en los programas de Office como Word, Power Point, Excel y de ofimática.

- Encriptación y desencriptación de ficheros con aplicaciones que generan contraseñas compartidas, por ejemplo: Secret Message Encrypt, Trillian, Letstalk IM, Surespot.
- Contratación del servicio web de mensajes privados, que integra en un enlace el dominio, id del mensaje y código, con la promesa que después de ver la información se destruye en automático sin dejar copia de seguridad, *por ejemplo:* Scrt.link, Qlink.it.

- No compartir el QR del contacto personal que se localiza en el perfil del usuario a terceros sin el conocimiento del titular.
- No compartir el QR de vinculación entre dispositivos a terceros, que propicie el inicio de sesión alterna de forma ilícita, sin el conocimiento del titular.
- No compartir código de verificación (PIN).
- Activar los mecanismos de privacidad de la cuenta, preestablecidos desde la aplicación y sitio web.
- Proteger el buzón de voz (ver figura 13).
- Nombrar a tus contactos sin referencias familiares, por ejemplo: mamá, papá, hijo(a), primo(a), u otras.
- Bloquear la pantalla con biometría de huella dactilar.

Figura 13. Buzón de voz.



Los ataques insistirán en medir la seguridad de las aplicaciones hasta encontrar una vulnerabilidad. A partir del compromiso que asumen los desarrolladores para crear entornos digitales seguros, se comparten acciones para activación de controles de privacidad por WhatsApp (ver figura 14).

Figura 14. Privacidad en WhatsApp.



Redes sociales

El uso de las aplicaciones que permiten las conexiones sociales, como Facebook, Instagram, TikTok, YouTube y similares, ha dejado expuesta la seguridad e integridad de las personas al convertirse en el medio digital más común para el intercambio de información. Esto ocasiona un exceso de confianza y la falta de una cultura digital de prevención que proteja la información sensible que circula en internet.

Facebook se encuentra entre las aplicaciones con mayores intentos de ataques por la información que contiene. Podemos indicar que el número de parches de seguridad corresponde a los intentos de penetración, manteniendo a la plataforma en un proceso de mejora continua constante. Por ello se sugiere:

- Verificar el URL: www.facebook.com en la barra del navegador, antes de ingresar la cuenta de correo y contraseña.
- Ingresar a la aplicación en la computadora o dispositivos móviles personales.
- Configurar adecuadamente la privacidad del perfil para controlar:
  - La visibilidad de las publicaciones, historias y reels.
  - Quién puede encontrarte mediante tu correo electrónico, número telefónico o motores de búsqueda.
  - Quién puede enviarte solicitudes de amistad, seguir tu perfil, etiquetarte o visualizar tu estado activo.
  - La información personal visible, como datos laborales, académicos, familiares, residencia, intereses y lugares destacados.
  - Los bloqueos de usuarios, mensajes y páginas.
  - La restricción del perfil para limitar la visualización del contenido a personas autorizadas.

- No guardar en el navegador las contraseñas.
- No dejar la aplicación con la sesión abierta cuando terceros tengan acceso al dispositivo.
- No acceder a enlaces de procedencia desconocida ni descargar archivos no confiables.
- No participar en trivias, juegos, sorteos u otras dinámicas que soliciten información personal o datos sensibles (nombre, correo, teléfono).
- No publicar capturas de pantalla, conversaciones o documentos obtenidos de plataformas basadas en inteligencia artificial, cuando contengan información personal, institucional o confidencial.
- Verificar que las fotografías y videos no expongan información sensible de forma involuntaria, como documentos, credenciales, gafetes, placas de vehículos, pantallas de equipos, domicilios u otros datos personales o de terceros.

- Verificar la autenticidad de publicaciones y notificaciones antes de interactuar con ellas.
- Evitar revisar perfiles que no quieres que se postulen como sugerencias de "Personas que quizás conozcas".
  - Aunque no hay pruebas de que visitar un perfil active las sugerencias de Meta, acciones como buscar el nombre de alguien o interactuar con contenido relacionado pueden ser interpretadas por el algoritmo como una señal de interés, aumentando la probabilidad de que esa persona aparezca entre tus recomendaciones, o incluso que tú aparezcas en las suyas.

En relación con el contenido digital que se comparte, es importante tomar conciencia de que no debe definir la vida privada de las personas, que internet es un entorno no controlado que difunde información a una comunidad virtual ilimitada, dejando expuesta la integridad de todos los participantes; por lo tanto, se sugiere:

- No publicar contenido que identifique a los familiares y amigos más cercanos.
- No anunciar desplazamientos, vacaciones o ausencias prolongadas.
- No exponer la ubicación del domicilio particular, laboral, escolar o los lugares que frecuenta, particularmente de los menores de edad.
- No evidenciar información que promedie el nivel socioeconómico y bienes patrimoniales.
- No etiquetar a contactos en publicaciones e imágenes sin previo consentimiento.
- Verificar que las fotografías y videos no expongan información sensible visible, como credenciales, gafetes, matrículas, documentos, pantallas de equipos o datos personales.

- Verificar la autenticidad de imágenes, audios y videos antes de compartirlos, considerando el uso de herramientas de inteligencia artificial para generar contenido falso.

Una buena gestión de contraseñas siempre será un mecanismo de seguridad que se puede aplicar mediante la activación de las siguientes prácticas:

- Proteger la cuenta: Contraseña y seguridad / Comprobación rápida de seguridad /Activa la autenticación en dos pasos,
- Cerrar sesión de forma remota: Cuenta /Contraseña y seguridad /Donde iniciaste sesión.
- Restablecer la contraseña: Cuenta /Contraseña y seguridad /Inicio de Sesión/Cambiar contraseña.
- Reportar actividad inusual: Cuenta/Contraseña y seguridad /Sí crees que hackearon tu cuenta.

La privacidad reduce el riesgo de acoso; sin embargo, el *stalkeo* es una práctica de observación virtual en donde el *stalker* analiza publicaciones para encontrar patrones de comportamiento y obtener información de interés. Por ello, antes de compartir información personal conviene reflexionar sobre quiénes te siguen o quiénes te persiguen, y decidir el propósito de la publicación, el momento oportuno y el tiempo determinado que permanecerá disponible. No obstante, el ataque también puede ser por fraude o extorsión, buscando una debilidad a través de la suplantación de identidad del perfil, por ejemplo:

- *Catfish:* es una estrategia de ingeniería social que realiza un fraude de identidad por redes sociales para engañar a la víctima, creando un perfil falso con imágenes y contenido a la conveniencia del delincuente, generalmente para ganarse la confianza del usuario y obtener información de primera mano, mediante la manipulación o amenaza.

- Suplantación de identidad*:* es un delito digital que realiza un perfil falso con contenido audiovisual lo más idéntico al personal, para estafar a víctimas en nombre del supuesto titular; en este caso se sugiere ingresar a la foto de portada/menú reportar/seleccionar cuenta falsa o página falsa.

Además de las vulnerabilidades expuestas en redes sociales, también se observa riesgo en el espacio de interacción virtual en donde los usuarios intercambian ideas y pensamientos sin restricciones a través del derecho de libertad de expresión, que enmarca nuestra Constitución. Sin embargo, el privilegio se limita cuando el contenido promueve actos que alteren el orden social señalados en los delitos de discriminación, difamación, acoso, prostitución, lenocinio, genocidio y feminicidio, entre otros.

Aunque a la víctima le asiste el derecho de ejercer las acciones legales por la vía civil o penal, con las evidencias digitales que correspondan también existe la posibilidad de denunciar el perfil o contenido directamente ante la aplicación, siguiendo las rutas siguientes:

- Foto de portada/menú reportar/acoso o bullying.
- Foto de portada/menú reportar/contenido inapropiado.
- Foto de portada/menú reportar/otro problema.

Correo electrónico

Es un canal de comunicación más robusto que la mensajería instantánea y las redes sociales; permite el envío masivo de mensajes electrónicos de gran tamaño a múltiples usuarios. Entre los proveedores de servicio más reconocidos se encuentran: Gmail, Yahoo y Outlook, con la integración de Live y Hotmail. Actualmente trabajan con protocolos de seguridad diferentes, pero a partir de nuevos esquemas de trabajo colaborativo, con base en el principio de la interoperabilidad en las comunicaciones, se esperan protocolos más reforzados.

Una de las bondades actuales del correo electrónico es que no hay una restricción en el número de cuentas que pueda crear un usuario; aun cuando estas sean personales o corporativas, las personas disponen de una suite de servicios por cada una, en las cuales se puede gestionar y almacenar información. Este último hecho posiciona este servicio como un objetivo de ataques informáticos, principalmente por la interacción humana, por ejemplo:

- Los accesos por correo electrónico se encuentran en riesgo cuando se ingresa en computadoras públicas o dispositivos ajenos al usuario. Para minimizar las consecuencias se sugiere realizar las siguientes acciones antes de abandonar el equipo:
  - Cerrar sesión.
  - Eliminar la cuenta del navegador.
  - Eliminar listas y recorridos de navegación.

  Para mayor seguridad, se recomienda previamente:
  - Activar mecanismos de autenticación multifactor, cuando el proveedor del servicio lo permita, para agregar una capa de protección ante accesos no autorizados.
  - Desactivar los recorridos antes de iniciar la navegación en internet.
  - Actualizar la contraseña posteriormente, manteniendo un alto nivel de seguridad.

- Cuando el equipo es personal se recomienda cerrar sesión eventualmente, para verificar el proceso de autentificación y también programar los tiempos en que se deban eliminar automáticamente los datos de navegación, sobre:
  - Historial.
  - Cookies y otros datos de sitios.
  - Archivos de imágenes en caché.
  - Contraseñas y otros datos de inicio de sesión.

- Datos para autocompletar formularios.
- Configuración de sitios.

- Los envíos de correos electrónicos son susceptibles al espionaje digital. Para reducir el riesgo se sugiere:
  - Enviar en modo confidencial, para que el correo no se pueda reenviar, copiar, imprimir o descargar por un tiempo definido y con la restricción de contraseña.
  - Encriptar los documentos anexos, con aplicaciones.

Figura 15. Técnicas de filtración por ingeniería social.



- Los fraudes por correos electrónicos siguen siendo la mayor fuente para acceder a datos personales, cuentas financieras y contraseñas de incautos, mediante técnicas de filtración: *Phishing, Smishing, Vishing, Spear Phishing* y *Whaling –véase glosario tiops de ataques por ingeniería social-,* que tienen diferentes alcances según la población objetivo (ver figura 15); para reducir el riesgo de ser víctima se sugiere:

- No ingresar a enlaces sin estar seguros del origen y destino, aunque aparente venir de contactos oficiales.
- Verificar los siguientes elementos en el contenido del correo que puede ayudar a determinar si es fraudulento: la calidad de la ortografía, logotipos, marcas y el dominio de la cuenta de donde proviene el correo.
- En los sitios web redireccionados, observar si cuenta con el candado de seguridad y protocolo HTTPS; aunque no es una garantía total reduce significativamente el riesgo.

Los correos electrónicos también han asumido el rol de cuen-tas de usuario en las plataformas digitales de servicios financie-ros, comercio electrónico, entretenimiento, educación y sociales, que se autentifican con una contraseña, las cuales se pueden visualizar en la configuración del navegador, desde la computadora o dispositivo móvil.

La concentración de cuentas por servicios digitales incrementa el riesgo de exposición de información sensible ante un acceso no autorizado, particularmente cuando el usuario proporciona, almacena o procesa documentos, conversaciones, datos personales o información confidencial en aplicaciones de inteligencia artificial.

Con la intención de optimizar los tiempos de acceso y búsqueda web, Google Chrome, Microsoft Edge, Mozilla Firefox y similares ofrecen el servicio de almacenar las contraseñas y el historial de navegación, como se cita a continuación:

- En Google Chrome: Ingresar a Configuración/ Autocompletar/Gestor de Contraseñas; en esta opción se puede ver el estatus de vulnerabilidad de las contraseñas, las almacenadas y las que nunca se guardan.
- En Edge: Ingresar a Configuración/Perfil/Contraseñas; en esta opción se pueden ver las contraseñas almacenadas y las que nunca se guardan.

Actualmente el navegador no es necesariamente inseguro; el problema es cuando:

- alguien tiene acceso al equipo desbloqueado;
- existe malware -*véase glosario tipos de malware*-;
- la cuenta del navegador está sincronizada.

Entonces, ¿por qué debo preocuparme de que las contraseñas estén almacenadas en el navegador?

La respuesta estaría en función del grado de vulnerabilidad y nivel de espionaje a cada sitio web registrado, así como del nivel de protección del dispositivo donde se utiliza el navegador.

¿Cuáles son los riesgos y las amenazas que se presentan?

- El acceso ilegal de terceros a los sitios o plataformas, usurpando la identidad del titular para acceder, modificar, agregar o eliminar la información privada.
- El acceso ilegal a las cuentas de correo electrónico para obtener la información de los contactos: nombre, correo electrónico, número telefónico, puesto y empresa; mediante la opción Ingresar a Configuración/ gestionar cuenta/ contactos y compartir/ contactos.

En las cuentas de correo electrónico que están relacionadas con las redes sociales, en ambiente web y en los dispositivos móviles, hay datos que se pueden verificar en el menú de configuración de cada una. Por ejemplo:

- En Twitter: Ingresar a la opción de Configuración/Tu Cuenta/Información de la Cuenta/ y ver el correo electrónico registrado.
- En Facebook: Ingresar a la opción de Información básica y de contacto del Perfil y ver el correo electrónico registrado.

Dispositivos móviles y computadores

Son dispositivos de procesamiento con conexión a internet, fuen-tes de información y canales de comunicación con otros medios de alojamiento digital, que requieren el resguardo lógico y físico, mediante las siguientes recomendaciones:

- Protección de pantalla con patrón de bloqueo, contraseña y métodos biométricos (reconocimiento facial y huella dactilar) (ver figura 16), requeridos al iniciar cada sesión de uso, mediante:
  - Configuración/ Contraseña y seguridad / pantalla de bloqueo-Cara-huella dactilar.

Figura 16. Controles biométricos



- Configurar el bloqueo automático de pantalla después de un periodo de inactividad, evitando el acceso no autorizado cuando el dispositivo queda sin supervisión.
- Protección de puertos USB a nivel BIOS, sistema o aplicación, para el control de acceso no autorizado de memorias, mediante:
  - La deshabilitación de los puertos USB, con el programa *regedit.exe, para* editar los registros en los servicios *USBSTOR* y cambiar el valor DWORD de 0 a 4.

  - La deshabilitación de los puertos USB, con el administrador de dispositivos, cambiando la configuración de los controladores del bus serie universal.
  - El bloqueo de los puertos, mediante aplicaciones, entre algunas alternativas existen las siguientes: USB loker, y USB block.

- Protección de todas las aplicaciones instaladas o de las seleccionadas, con contraseña, brindando mayor seguridad a la banca móvil, redes sociales y demás aplicaciones, en el caso de extravío o robo.

  - Mediante: Configuración/Aplicaciones /Bloqueo de Aplicaciones.

- Protección ante una probable clonación del dispositivo, sin conocimiento y autorización.
- Realizar respaldos periódicos de la información importante en medios seguros o servicios de almacenamiento, en el caso de daño físico, ransomware o robo.
- Activar el cifrado del almacenamiento del dispositivo para proteger la información contenida ante pérdida, robo o acceso no autorizado.
- Protección contra la suplantación de tarjeta SIM (SIM swapping), mediante:
  - El registro de un PIN de seguridad con el operador telefónico para evitar modificaciones no autorizadas de la tarjeta SIM.

- Protección del dispositivo por el rastreo del International Mobile Equipment Identity (IMEI), que es un número de identificación único del dispositivo móvil, que en estado activo puede realizar llamadas, enviar mensajes y utilizar aplicaciones web, con la colaboración de la tarjeta SIM (ver figura 17), mediante:

- El registro del IMEI en un lugar seguro diferente al dispositivo, para facilitar el reporte ante pérdida o robo.

Figura 17. International Mobile Equipment Identity.



Además, se presentan algunas técnicas para identificar el IMEI:

- Por asistencia telefónica marca *#06#, y en el caso que tenga dos módulos para tarjeta SIM, se proporcionarán dos números IMEI.
- Por configuración del dispositivo:
  - Android. Configuración/Acerca del Teléfono/Todas las especificaciones /Estado/IMEI.
  - IOS. Ajustes/General /Información/IMEI.

- Por internet:
  - Android. Cuenta Google/Seguridad/Tus dispositivos/Encontrar Mi Dispositivo/IMEI.
  - IOS. iCloud/Configuración del dispositivo/IMEI.

Entre las acciones más recurrentes sobre la gestión del IMEI se encuentran las siguientes:

- Activación del Rastreo de Celular, por medio de la función de Encontrar Mi Dispositivo,
  - o Android:

Cuenta Google/Seguridad/Tus dispositivos/Buscar en el dispositivo deseado/Mapa con la ubicación más próxima de la última conexión registrada.

- Cuando se activa la función de Encontrar Mi Dispositivo, el teléfono recibe una notificación de ubicación.
- Se puede elegir Reproducir Sonido que activa una alerta por 5 minutos, Bloquear Dispositivo o Borrar Datos

- Activación y Desactivación del Historial de Ubicaciones de forma discrecional, derivado de:
  - o Almacena información de los sitios que visita el usuario, mediante el rastreo GPS de los dispositivos.
  - o Guarda la ubicación en tiempo real durante el servicio de aplicaciones asociadas a la cuenta Google, y en algunas ocasiones, configuraciones incorrectas de privacidad o permisos excesivos pueden permitir el acceso prolongado a la ubicación.

- Traza un mapa con las rutas recorridas y puntos registrados.

Figura 18. Función Encontrar dispositivo.



Aplicaciones

Las aplicaciones son programas de software que permiten la interacción con el usuario, inclusive también interactúan con los recursos del sistema operativo, procesador, memoria y almacenamiento. Se les conoce como la parte lógica del sistema y haciendo alusión al término se han convertido en el elemento más vulnerable en términos de seguridad.

El desarrollo de aplicaciones modernas basadas en arquitecturas cliente-servidor, servicios web, API REST y tecnologías Full Stack ha incrementado significativamente la superficie de ataque sobre los sistemas de información. Por ello, la ciberseguridad debe incorporarse desde las etapas iniciales del diseño y desarrollo del software, mediante controles de autenticación, autorización, cifrado de la información, validación de entradas y gestión segura de sesiones, bajo principios como Security by Design y Defense in Depth.

Las medidas de prevención para fortalecer la comunicación electrónica y digital, entre las redes sociales, financieras, legales, administrativas, juegos de azar, entretenimiento, buscadores y navegadores, pueden ser:

- Instalación de antivirus como mecanismo de autodefensa, con la opción de seleccionar el formato de prueba, gratuito o premium, considerando la relación directa entre prestaciones y nivel de protección. Es decir, ponderar la seguridad ante el presupuesto.
  - Opciones: AVG, Norton, McAfee y NOD32.

- Actualización de software que sugieren los desarrolladores para mantener la convivencia tecnológica con otros programas que interactúan en el sistema de arranque o ambiente web; mediante la instalación automática o manual de fragmentos de código que mejoran el rendimiento de los componentes y aumentan la seguridad del programa, incluyendo los parches que mitigan errores.
-

Aplica a todos los programas de software:

- Redes sociales, mensajería instantánea, correo electrónico.
- Sistemas operativos, programas de ofimática, diseño, desarrollo.
- Navegadores, buscadores.
- Antivirus, entre otros.

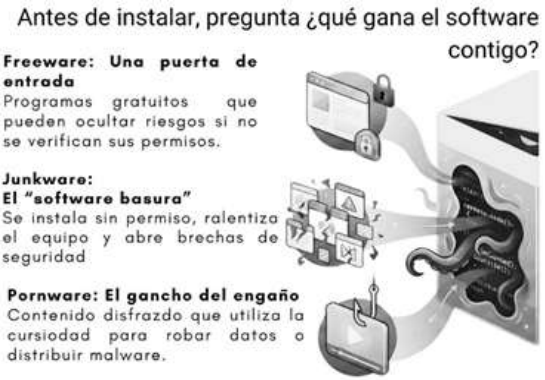
- Bloqueo o desinstalación de programas nativos o *Junkware* preinstalados de fábrica por política de los desarrolladores, que tienen la cualidad de consumir mayores recursos, afectando el rendimiento del dispositivo, modificando las configuraciones del sistema, recolectando datos del usuario y perfil de navegación (ver figura 19).

Figura 19. Junkware



- Verificar las características y condiciones de uso del software gratuito *Freeware* y *Shareware –véase glosario tipos de malware-*. Aunque no constituye software malicioso por definición, el *freeware* puede incorporar funciones de recopilación de información, publicidad integrada o la instalación de componentes adicionales que comprometan la privacidad y seguridad del usuario (ver figura 20).
- Evitar la instalación de aplicaciones con contenido para adultos o enlaces engañosos utilizados como anzuelo, para la distribución de código malicioso, modificación del navegador o instalación de software no autorizado.

Figura 20. Freeware



- Descarga exclusiva en sitios y tiendas en línea, reduciendo el riesgo de instalar bajo engaño programas maliciosos que ofrecen incorporar nuevos servicios, con la falsa promesa de seguridad y privacidad de datos. Se sugiere:
  - No ingresar a sitios que ofrecen descargas de aplicaciones gratuitas
  - No ingresar a tiendas en línea que no se encuentran en la suite de aplicaciones de tu proveedor de servicio.

Como medida de prevención, antes de instalar una aplicación conviene preguntarse: ¿qué gana el software contigo? La respuesta puede encontrarse en la información que recopila, los permisos que solicita, la publicidad que incorpora o los servicios adicionales que instala; por ello, es indispensable verificar siempre su procedencia y políticas de privacidad antes de su instalación.

- No escanear códigos QR de procedencia desconocida, sin verificar previamente su autenticidad y el sitio al que direccionan, debido a que pueden redirigir a páginas fraudulentas, iniciar la descarga de aplicaciones maliciosas o capturar información personal.
- Actualización periódica de las contraseñas.
- Revisar las políticas de privacidad y permisos solicitados por las aplicaciones, especialmente aquellas basadas en inteligencia artificial, evitando proporcionar información personal, institucional o confidencial sin autorización.
- Revisión de permisos otorgados a las aplicaciones, limitando el acceso a cámara, micrófono, ubicación, contactos y archivos únicamente cuando sea necesario para su funcionamiento.
- Eliminación o desinstalación de aplicaciones que no sean utilizadas, debido a que pueden representar riesgos por falta de actualización o mantenimiento del desarrollador.
- Activación de mecanismos de autenticación multifactor en aplicaciones que permitan esta función, especialmente aquellas relacionadas con información financiera, laboral o personal.

Navegación y entornos web

La mayoría de los proveedores de servicios web mantienen un registro de la actividad realizada por el usuario con fines de funcionamiento, personalización y seguridad; por ello, conviene revisar periódicamente dicha información y administrar su conservación conforme a las necesidades de privacidad. En este contexto, un entorno web seguro debe contar, entre otras, con las siguientes prácticas de seguridad:

Las extensiones, plugins y aplicaciones son complementos que incrementan la funcionalidad de los navegadores; algunas se instalan automáticamente y otras a selección del usuario. Como medida preventiva, se sugiere:

- Supervisar periódicamente cuáles están activados, eliminar los que no se utilizan y verificar los permisos que conservan sobre las cuentas vinculadas.
    - Las extensiones de Google Chrome se encuentran en el sitio oficial y se activan en el menú del navegador.
    - Los *pluggins* pueden ser administrados por Shareaholic, plugin de Facebook y Join.chat.
    - Las aplicaciones en redes sociales pueden ser eliminadas a partir de la revocación de los permisos en la cuenta.

- Revisar la actividad registrada por las cuentas utilizadas en los servicios web, eliminando aquella que no sea necesaria y configurando su eliminación automática.
- Supervisar los dispositivos con sesiones activas y cerrar aquellas que no correspondan al usuario o cuya actividad no pueda ser identificada.
- Revisar los permisos otorgados a aplicaciones y servicios de terceros vinculados a las cuentas, revocando aquellos que ya no sean necesarios.

- Ejecutar las herramientas de verificación de seguridad que ofrecen los proveedores de servicios web para identificar configuraciones inseguras, dispositivos conectados y actividades inusuales.

Los elementos propios de la navegación web, como el dominio del sitio, el protocolo HTTPS, los permisos del navegador, las notificaciones y las descargas, también desempeñan un papel importante en la seguridad; para ello, se recomienda incorporar las siguientes prácticas:

- Verificar que el dominio del sitio web corresponda al servicio oficial, antes de ingresar credenciales, datos personales o información financiera.
- Comprobar que el sitio utilice el protocolo HTTPS y un certificado digital válido, considerando que estas medidas fortalecen la seguridad de la comunicación, aunque no garantizan por sí mismas la legitimidad del sitio.
- Configurar la red inalámbrica utilizando los protocolos de seguridad WPA2 o, preferentemente, WPA3, ya que fortalecen la autenticación y el cifrado de las comunicaciones entre los dispositivos y el punto de acceso. Asimismo, se recomienda evitar redes que continúen utilizando protocolos obsoletos como WEP o WPA, debido a las vulnerabilidades conocidas que comprometen la confidencialidad de la información transmitida.
- Modificar el nombre de la red inalámbrica (SSID) predeterminado por el fabricante, evitando utilizar nombres que revelen información sobre la organización, el domicilio, el proveedor del servicio, el modelo del equipo o cualquier otro dato que facilite las actividades de reconocimiento por parte de un posible atacante.
- Cambiar las credenciales de administración predeterminadas del router o punto de acceso inalámbrico, estableciendo nombres de usuario y contraseñas robustas y únicas que impidan el acceso no autorizado a la configuración del dispositivo.

- Mantener actualizado el firmware del router o punto de acceso inalámbrico mediante la instalación de las actualizaciones de seguridad proporcionadas por el fabricante, con la finalidad de corregir vulnerabilidades conocidas y fortalecer la protección de la red.
- Verificar si el navegador almacena automáticamente las contraseñas y, cuando el computador o dispositivo sea compartido o de uso público, desactivar dicha opción.
- Cerrar la sesión al finalizar la operación en plataformas, páginas o sitios web donde se comparta información personal, financiera o confidencial.
- No autorizar notificaciones de sitios web cuya procedencia se desconozca, revocando los permisos otorgados a páginas que ya no sean utilizadas.
- Descargar archivos, programas y actualizaciones exclusivamente desde los sitios oficiales del desarrollador o de proveedores reconocidos, evitando enlaces de terceros que puedan distribuir software malicioso.
- Supervisar los permisos otorgados a los sitios web, limitando el acceso a la cámara, micrófono, ubicación, portapapeles, notificaciones y otros recursos del dispositivo, únicamente cuando sean necesarios.
- Cuando se utilicen servicios de almacenamiento o aplicaciones basadas en la nube (Cloud Computing), verificar que las cuentas cuenten con autenticación multifactor, revisar periódicamente los permisos de acceso a los archivos compartidos y evitar almacenar información sensi-ble en servicios que no ofrezcan garantías suficientes de seguridad y privacidad.
- No asumir que la navegación en modo incógnito proporciona anonimato o privacidad absoluta; su función consiste en reducir los registros locales del historial de navegación, sin impedir que los sitios web y los proveedores de servicios de internet puedan recopilar información (ver figura 21).

- Evitar ingresar información confidencial en sitios web que presenten errores de funcionamiento, mensajes de advertencia del navegador, certificados digitales inválidos o comportamientos inusuales, ya que podrían ser indicios de vulnerabilidades o de un intento de suplantación del servicio.

Figura 21. Modo incógnito.



Las aplicaciones web modernas sustentan una gran parte de los servicios digitales utilizados diariamente, como plataformas de comercio electrónico, banca en línea, sistemas académicos, servicios gubernamentales y aplicaciones empresariales.

En la actualidad, una proporción importante de estos servicios opera sobre infraestructuras de computación en la nube (Cloud Computing), lo que permite ofrecer mayor disponibilidad, escalabilidad y acceso remoto; sin embargo, también exige fortalecer los controles de autenticación, cifrado, gestión de accesos y protección de la información almacenada.

Debido a que estas soluciones intercambian información de manera continua entre el navegador, los servidores y las bases de datos, constituyen uno de los principales objetivos de los ataques informáticos. Los proveedores de servicios web incorporan mecanismos de seguridad para la protección de las cuentas; sin embargo, su eficacia depende de que el usuario los configure y mantenga activos, de acuerdo con su nivel de riesgo y necesidades de seguridad.

En consecuencia, la seguridad de un entorno web no depende únicamente de los mecanismos implementados por los proveedores del servicio, sino también de la adopción de buenas prácticas por parte de los usuarios y de la implementación de controles de seguridad durante el diseño, desarrollo y mantenimiento de las aplicaciones, con el propósito de reducir la superficie de ataque y proteger la confidencialidad, integridad y disponibilidad de la información –*véase glosario la triada de la ciberseguridad*-.

Medidas para la mitigación del Riesgo

La implementación de controles de seguridad constituye un elemento esencial para reducir la probabilidad de materialización de los riesgos y disminuir el impacto de los incidentes de seguridad que afectan a la infraestructura tecnológica. Si bien no existe una medida única capaz de eliminar todos los riesgos, la aplicación de controles fortalece la confidencialidad, integridad y disponibilidad de la información, contribuyendo al fortalecimiento de la ciberresiliencia institucional (*véase glosario, taxonomía de la ciberseguridad)*.

En la tabla 13 se presentan algunas de las principales medidas utilizadas para la mitigación del riesgo en los entornos digitales.

Entre las principales estrategias de mitigación se encuentra la protección de los datos, cuyo objetivo es preservar la confidencialidad, integridad y disponibilidad de la información, ante las amenazas de espionaje y robo, especialmente en transferencias y almacenamiento.

Una de las técnicas más utilizadas para este fin es el cifrado de datos, que consiste en transformar la información mediante algoritmos criptográficos para que únicamente las personas autorizadas puedan acceder a su contenido.

Entre los algoritmos de cifrado más utilizados se encuentra el Advanced Encryption Standard (AES), ampliamente adoptado para proteger bases de datos, archivos y otra información almacenada. Asimismo, herramientas como VeraCrypt permiten cifrar

discos completos, particiones y dispositivos de almacenamiento, fortaleciendo la protección de la información frente a accesos no autorizados.

Tabla 13. Medidas para la mitigación del riesgo.

No.	Medida	Propósito
1	Segregación y segmentación de redes	Limitar el acceso a la red interna y contener posibles ataques a una sección de la red sin comprometer otras áreas.
2	Análisis y escaneo de vulnerabilidades	Identificar y remediar vulnerabilidades antes de que sean explotadas.
3	Pruebas de penetración (pentesting)	Evaluar la seguridad de la infraestructura mediante la simulación de ataques controlados e identificar oportunidades de mejora.
4	Monitoreo y auditoría de seguridad	Detectar y responder oportunamente a incidentes de seguridad.
5	Concientización y capacitación en seguridad	Reducir el riesgo de ataques de ingeniería social, como el phishing, y mejorar la cultura de seguridad.
6	Backups y recuperación ante desastres	Asegurar que los datos críticos estén protegidos y puedan ser recuperados en caso de un incidente.
7	Uso de firewalls y sistemas de detección/prevención de intrusos (IDS/IPS)	Controlar y monitorear el tráfico de red para identificar y detener actividades sospechosas.
8	Cifrado o encriptación de datos	Proteger la confidencialidad e integridad de los datos, tanto en tránsito como en reposo.
9	Gestión de parches y actualizaciones	Reducir la exposición a vulnerabilidades conocidas en sistemas operativos y aplicaciones.
10	Control de acceso y autenticación	Asegurar que solo el personal autorizado tenga acceso a ciertos sistemas y datos.

En conjunto, la implementación de controles de seguridad y medidas de mitigación del riesgo fortalece la protección de la información y mejora la capacidad de las organizaciones para enfrentar las amenazas del entorno digital.

Capítulo III.

Cultura de Seguridad, Factor Humano y Protección de Datos

Introducción

La transformación digital promueve la incorporación de las tecnologías de la información en los procesos organizacionales; no obstante, la seguridad puede verse comprometida, ya que no existe una garantía absoluta de protección. Esta limitación de la tecnología ha sido atribuida a Roger Needham y retomada por Bruce Schneer en Secrets and Lies: Digital Security in a Networked World (2000, p. xii), quien señala: "Si piensas que la tecnología puede resolver tus problemas de seguridad, entonces no entiendes los problemas y no entiendes la tecnología". Esta cita expone que las soluciones tecnológicas pueden presentar vulnerabilidades o generar mecanismos susceptibles de ser explotados mediante otras tecnologías o técnicas.

Sin embargo, el factor humano es el principal elemento que influye en la protección de la información y en la resiliencia de las organizaciones, lo que hace indispensable complementar las soluciones tecnológicas con estrategias de gestión de riesgos, políticas de seguridad, controles organizacionales y la capacitación continua de los usuarios (Ghafoori, A., et al., 2024). En este

sentido, (Mitnick, 2002) destaca la importancia del factor humano en la seguridad de la información, al señalar que este constituye uno de los elementos más vulnerables de la seguridad. Esta perspectiva permite reconocer que las medidas tecnológicas, por sí solas, no garantizan la protección de la información, por lo que deben complementarse con la participación responsable, la capacitación y la concientización de los usuarios.

Este capítulo se enfoca en el papel del factor humano como un componente débil de la ciberseguridad, abordando temas relacionados con la cultura de seguridad, la protección de datos, la privacidad, la ingeniería social, la ética digital y las buenas prácticas de seguridad. Asimismo, considera dos casos de análisis para la fortalecer la cultura de ciberseguridad.

Como propuesta de valor incluye manual de políticas de seguridad informática.

Buenas prácticas con contraseñas

La seguridad informática se encuentra en un punto crítico por el grado de incidencia que han alcanzado los actos de ciberdelincuencia; ante este fenómeno:

- Las industrias de desarrollo en tecnologías crean, implementan, evalúan y actualizan constantemente los mecanismos de seguridad que tienen los sistemas, como un proceso de mejora continua para la prevención o disminución de un ataque.
- Las empresas asumen con responsabilidad social, estrategias de prevención y esquemas de atención, para fortalecer los puntos vulnerables, disminuir riesgos y afrontar la recuperación en el menor tiempo posible.
- La academia promueve programas de capacitación orientados al fortalecimiento de habilidades y destrezas para la formación técnica de profesionales en ciberseguridad.

- El órgano jurídico impulsa iniciativas de ley y promulga reformas para abatir las lagunas legales y brindar mayor cobertura a los derechos y garantías individuales constitucionales.

Sin embargo, estas acciones enfrentan una amenaza en común: el factor humano, que ante la falta de atención de las medidas de prevención abre una brecha de oportunidades a la ciberdelincuencia (Handri, E., et al., 2024) con daños a la protección de datos personales y privacidad de la información que de manera colateral afectan la estabilidad social y económica, así como la integridad emocional y, en algunas situaciones más específicas, exponen a la víctima a un riesgo físico (ver figura 22).

Figura 22. El factor humano.

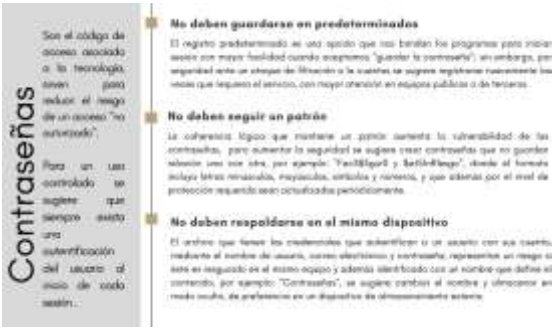


En seguimiento, se exponen buenas prácticas de ciberseguridad (BPC) sobre la creación y gestión de contraseñas que pueden ser un referente para la cultura digital del actual modelo tecno-social; así como las amenazas que se pueden presentar.

Código de acceso

Las contraseñas son el código de acceso que autentifican al usuario para el inicio de una sesión en computadoras, celulares, tabletas, sistemas, sitios y páginas web, así como en aplicaciones y plataformas; sin embargo, existen prácticas que deben erradicarse para proveer un nivel de seguridad básico (ver figura 23):

Figura 23. Nivel de seguridad básica en contraseñas.



- No deben guardarse en predeterminados, aunque es una opción viable que nos permite optimizar el tiempo y acceder con mayor facilidad en cada inicio de sesión, por ser una acción que representa un alto riesgo ante un posible ataque de malware a las cuentas de los usuarios.
- No deben seguir un patrón que permita la deducción lógica de otras cuentas, por ejemplo: *Face123, Twitter123, Sat123*; esto ocasiona mayor vulnerabilidad al momento de usurpar la identidad del usuario.
- No deben respaldarse en archivos que se almacenan en el mismo dispositivo; cuando las contraseñas se guardan en el mismo disco duro o memoria se puede acceder fácilmente a ellas, además se incrementa el riesgo si el nombre denota el contenido y el formato es editable, por ejemplo: *contraseñas.txt.* En ocasiones se elige ocultar el archivo; sin embargo, no es una medida infalible de revertir. Esto se realiza como se presenta a continuación:

- Menú propiedades, opción/atributos/oculto.
- Para revertir: menú Ver del explorador de Windows y elegir Mostrar elementos ocultos.

Registro y almacenamiento de contraseñas

Las contraseñas, al ser registradas en el sistema operativo y navegadores web, se convierten en un activo codiciable por personas que buscan la manera de ingresar ilícitamente a los archivos de sistemas para sustraerlas junto con las cuentas de usuarios, a través de las siguientes rutas de almacenamiento:

- Microsoft Edge: Seleccionar configuración, opción/perfiles/contraseñas.
- Chrome: Seleccionar configuración, opción/Autocompletar y contraseñas/Administrador de contraseñas de Google/Revisión.
- Windows: Seleccionar Panel de Control/Cuenta de usuario/Administrar credenciales.

La obtención de forma ilegal de las credenciales de autentificación permite a los delincuentes ingresar a correos electrónicos, sitios web o aplicaciones digitales; a partir de esta acción pueden sustraer información sensible o realizar procedimientos sin el consentimiento ni autorización de las víctimas.

Tipos de acceso no autorizados

Entre las formas de acceso no autorizadas a las cuentas y contraseñas de los titulares por parte de terceros, se pueden mencionar la usurpación de identidad adquirida por estafas con estrategias de ingeniería social y el robo de datos personales mediante la filtración de malware en memorias extraíbles o dispositivos móviles que se transfieren por puertos USB y bluetooth. Esto incluye la depuración de la basura tecnológica para obtener las credenciales de autentificación. Para una mejor comprensión se describe enseguida:

- Por estafas con ingeniería social

Son estrategias sociales orientadas a la estafa digital a través de sorteos, promociones, rifas y regalos de productos o servicios, que crean un escenario falso de oportunidad a la víctima, para solicitar a partir del engaño las contraseñas e información confidencial que comprometen la revelación de la identidad y, en algunos casos, la pérdida de recursos económicos.

Las técnicas que se emplean para contactar con los usuarios se llaman: *phishing, vishing, smishing* y *qrshing,* que utilizan mensajes, imágenes, audios, videos y códigos QR, distribuidos por correos electrónicos, redes sociales y aplicaciones de mensajería. Todas ellas se caracterizan por contener direcciones de sitios o páginas web apócrifas que direccionan a formularios de datos que exhortan al usuario para compartir voluntaria e incautamente datos personales. Inclusive, pueden tener un nivel de coerción, obligando al usuario bajo presión a entregar sus credenciales de autentificación.

Es por ello que se recomienda:

- No ingresar en los enlaces, direcciones o URL que se incluyan en los mensajes de texto, audio e imágenes de dudosa procedencia.
- No proporcionar información en los formularios que no sea certificados o de validez oficial.
- No compartir con otros contactos, para evitar el efecto cadena.

Sin embargo, este fenómeno social toma mayor alcance cuando además de los enlaces incluyen archivos con malware, creando un mecanismo de alta intrusión a nivel software.

- Por filtración de malware

El troyano es un programa malicioso con la función de extraer contraseñas y cuentas de usuario del ordenador; incluyendo controladores del sistema, dispositivos, red e internet, por medio de la filtración por correo electrónico, redes sociales y aplicaciones.

Partiendo de la premisa de que la activación requiere de la intervención humana, se recomienda:

- No hacer descarga y apertura de archivos que se ignore su procedencia o se desconfíe del remitente.
- No seleccionar imágenes o símbolos anexos a los mensajes, que se desconfíe del propósito o la existencia de una URL enmascarada.

No obstante, las medidas de prevención de filtración del troyano, también existe el *keylogger* como otra variante de malware que se distingue del anterior, por tener en su programación la función de registrar las pulsaciones realizadas en el teclado en tiempo real, dejando al descubierto lo que se escribe en una sesión activa, inclusive caracteres especiales, impresiones de pantalla y selecciones del mouse. De esta manera obtiene los nombres de usuario, contraseñas, números de tarjetas, CURP, FIEL y otros más que almacena temporalmente en un fichero de texto plano o encriptados hasta el momento en que son recuperados (ver figura 24).

Figura 24. Keylogger



Sin embargo, las contraseñas que están protegidas por el proceso de autentificación con el multifactor (MFA) tienen

una capa de seguridad que exige la verificación de la identidad en un segundo plano, es decir, vía telefónica o correo alterno, convirtiendo esta medida de prevención como la única protección, siempre y cuando se encuentre activada en Google, como se indica a continuación:

- Ingresa a https://myaccount.google.com/security
- Selecciona Seguridad
- Selecciona Cómo acceder a Google
- Elige Verificación en 2 pasos y sigue las instrucciones

Al igual que el anterior, la activación del keylogger requiere la participación humana; es por ello que además de las anteriores recomendaciones se incorporan las siguientes:

- No ingresar memorias HDMI, USB, SD y SDXC, de las cuales se desconozca o desconfíe del propietario.
- No ingresar datos sensibles en teclados con la apariencia que han sido adaptados con fines fraudulentos.

Definitivamente, la falta de un adecuado control de acceso sobre los puertos USB del ordenador facilita la filtración del malware. Este se ejecuta automáticamente al ingresar el dispositivo, sustrayendo los datos sensibles sin la autorización y conocimiento del usuario propietario, mediante un proceso de depuración del código fuente en el sistema comprometido (*debugging*), con la finalidad de exportarlos cuando se retire el dispositivo en ficheros html, pdf, jpg o txt.

Ante la amenaza de un ataque se recomienda:

- Autoexplorar la ruta básica con los programas: rubber ducky y usb dumper, ambos con interfaz USB.
- Diseñar una prueba de penetración con la plataforma P4wnP1 A.L.O.A. aplicada a Raspberry Pi.
- Monitorear el acceso de todos los dispositivos USB: *USBDeview* y *Device Manager.*

Ahora bien, girando la perspectiva de una filtración de malware al ordenador, podemos señalar el robo de información a través la conexión de dispositivos en tomas de corriente públicas con acceso USB que han sido alteradas a nivel firmware, en donde el chipset incluye sentencias programadas con el propósito de extraer datos sensibles y dirigirla a ficheros controlados que permanecerán en la tarjeta esperando ser recuperados, después de que se retiren los dispositivos vulnerados. Por ello, se recomienda:

- No conectar celulares, tabletas o cualquier dispositivo móvil a tomas de corriente pública con acceso USB.

Así también, la tecnología inalámbrica de corto alcance tiene un espacio cuando por medio del Bluetooth se emparejan dos dispositivos sin necesidad de una conexión física o dirección lógica y, mediante estrategias de *Bluejacking* o *Bluesnarfing,* se fil-tran sentencias de ataque para la sustracción de datos sensibles sin la aprobación o conocimiento de la víctima. En consecuencia, se recomienda:

- Desactivar la conexión y la visibilidad Bluetooth.
- Activar la alerta de conexión de terceros.
- Supervisar periódicamente los dispositivos sincronizados.
- No realices transferencias de archivos de fuentes desconocidas o ficheros con contenido sospechoso.

Entonces, aun con el esfuerzo de erradicar las vulnerabilidades, siempre existirá la probabilidad de tener comprometidos nuestros dispositivos, ante esta situación se realiza el siguiente planteamiento:

- ¿Hay alguna forma por la cual podamos saber sí estamos infectados?

- Sí, por medio del rastreo de programas maliciosos, mediante el administrador de tareas y administrador de aplicaciones para identificar los procesos de inicio de sesión en Windows no autorizados y aplicaciones duplicadas.

A partir del hallazgo se realizan las siguientes acciones de contención:

- Finalizar la tarea duplicada.
- Desinstalar la aplicación duplicada.
- Proteger los puertos USB.
- Actualizar las contraseñas.
- Actualizar el antivirus.

- Por depuración de basura digital.

La obtención de datos sensibles de autentificación de los usuarios se realiza sobre la depuración de la basura tecnológica, mediante un proceso que tiene el grado mínimo de intrusión porque la revisión se encuadra en los desechos, pero con un alto grado de invasión a la privacidad.

La sustracción de datos se realiza acorde a los resultados de la restauración de unidades de memoria o chipset de los dispositivos que han sido descartados y tirados a los contenedores o recolectores de basura de manera voluntaria por parte de los titulares, generalmente por estar obsoletos, descompuestos o rotos; incluyendo aquellos que se encuentran actualizados, pero fueron robados o extraviados.

Las técnicas de cómputo forense encuentran aplicación en la recuperación de datos, donde la habilitación de los dispositivos para acceso a los datos depende exclusivamente del propósito de los usuarios. Entre las acciones más recurrentes se encuentran:

- La restauración de contraseñas y actualización de controladores.
- La habilitación de particiones (sectores y pistas), cabezales y tarjetas.
- La clonación de discos duros con fallos, mediante herramientas que permiten la recuperación de la información:
  - *Deep Spar Disk Imager y R-Studio*

Casos de análisis para la cultura de ciberseguridad

Caso 1. ¿El derecho humano de acceso a internet autoriza el uso de una red WiFi privada sin consentimiento?

Reflexión

¿Hasta dónde llega el derecho humano de acceso a internet y dónde comienza la responsabilidad de respetar la infraestructura digital y la propiedad privada?

En México, no existe un tipo penal específico que sancione de manera autónoma el acceso no autorizado a una red WiFi privada y contraseña del modem. Al no sancionarse, depende de nosotros vigilar la seguridad de nuestros equipos y sobre todo de nuestra información, porque no hay sistema infalible a un ataque cibernético.

Cuando se trata de identificar a quién pertenece la señal de internet de un hogar o de un negocio que se encuentra en el área electromagnética, se identifica a la persona física o moral que figura como suscriptor en la celebración del contrato mercantil con el concesionario de la red, al cual se le otorga la responsabilidad de las obligaciones y el derecho de los beneficios en la prestación del servicio e infraestructura de telecomunicaciones. En contraparte, al individuo que realiza actos ilegales para obtener gratuitamente el usufructo de los beneficios, a través de la sustracción de la señal WiFi y desencriptación de la contraseña de seguridad, se le denomina *ciberdelincuente.*

En esta relación, el objeto en común es la señal inalámbrica WiFi, que técnicamente representa un Service Set Identifier (SSID) en la conexión a internet que se encuentra asegurado con un código encriptado, y que se somete a pruebas de penetración hasta lograr el acceso no autorizado, convirtiendo el acto en un hecho ilegal.

Es interesante conocer la declaratoria que realiza la ONU mediante la Comisión de Derechos Humanos en aras de establecer que el acceso a internet sea considerado un derecho básico de todos los seres humanos: La promoción, protección y disfrute de los derechos humanos en internet (CDH, 2018).

Esta condición se proclama con la intención de promover el uso del mismo, a manera de un mecanismo confiable y seguro para la protección de las garantías individuales de los usuarios en línea, incluyendo la privacidad de datos, y una estrategia que reduzca la brecha digital y sus implicaciones en el desarrollo sostenible (ver figura 25).

Figura 25. Acceso a internet como derecho humano.



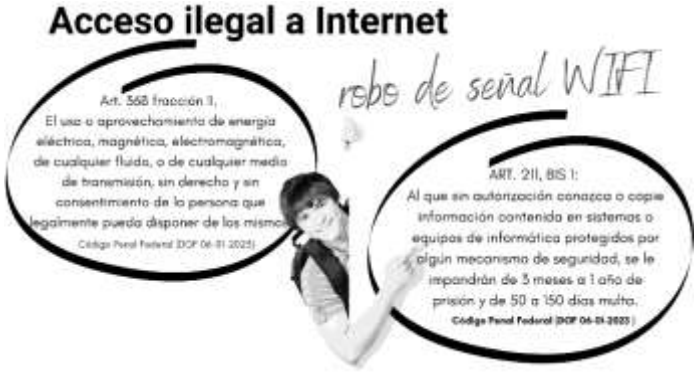
El derecho constitucional señalado en el artículo 6, en atención al acceso a internet, establece este acceso como un medio que acompaña a la garantía de la expresión de ideas de manera libre y responsable y el derecho a la información.

Ambos pueden ser desvirtualizados con la objeción del contexto general, creando una falacia del acto imputable de acceder a la señal WiFi de un tercero sin su consentimiento, interpretando erróneamente el término de acceso a internet como derecho humano, como justificante permisible de actividades ilícitas de hackeo.

De esta manera, la expresión gira en torno a su aplicación sobre la base jurídica nacional, descartando contundentemente el amparo al acceso no consensuado a redes privadas; con la excepción de las redes públicas, que permiten un servicio limitado o pasivo, en atención a las políticas públicas del gobierno.

Por lo tanto, todo individuo que accede ilegalmente a internet, violando los mecanismos de seguridad de dispositivos y programas, se entenderá como un robo de señal WiFi y contraseña del módem (ver figura 26), de acuerdo con el artículo 368 fracción II del Código Penal Federal (CPF, 2026): "El uso o aprovechamiento de energía eléctrica, magnética, electromagnética, de cualquier fluido, o de cualquier medio de transmisión, sin derecho y sin consentimiento de la persona que legalmente pueda disponer de los mismos".

Figura 26. Acceso ilegal a internet.



Y el Art. 211 bis 1, previa interpretación del verbo *conocer* a descifrar para el acceso ilícito a sistemas y equipos de informática: "Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa" (CPF, 2026).

Ahora bien, se presenta otra arista sobre el acceso a internet que trata de redimir la acción fraudulenta, con una exposición de motivos que observa las redes identificadas como intrusivas del espacio digital del usuario, mismas que son detectadas como redes disponibles, por el sistema operativo, adaptador y tarjeta de red, sin ningún un proceso de rastreo.

Con la intención de argumentar la postura legal sobre las redes inalámbricas, se realiza el siguiente cuestionamiento: ¿por qué mi señal de internet se observa en los equipos circunvecinos?, con la lógica de que la visualización aumenta la probabilidad de un acceso no autorizado; y en la misma línea se cuestiona: ¿por qué no aplicar el derecho a la privacidad digital y crear protocolos aplicados a las concesionarias para ocultar las redes inalámbricas en otros equipos? Definitivamente, estas inquietudes reflejan vulnerabilidades que aumentan el riesgo de espionaje de datos, más allá de un beneficio económico por gozar gratuitamente de internet.

Sin embargo, para una mejor comprensión de las obligaciones del acceso y la interconexión que estipula la Ley Federal de Telecomunicaciones y Radiodifusión (2021), se citan los artículos 124 y 125:

Los concesionarios que operen redes públicas de telecomunicaciones deberán adoptar diseños de arquitectura abierta de red para garantizar la interconexión e interoperabilidad de sus redes y los que operen redes públicas de telecomunicaciones estarán obligados a interconectar sus redes con las de otros concesionarios en condiciones no discriminatorias, transparentes y basadas en criterios objetivos.

Es importante agregar que no es permitido por la misma normatividad fabricar y comercializar dispositivos que bloqueen o inhiban las señales de transmisión de datos, con excepciones señaladas en el Art. 190 Bis; de lo contrario, el concesionario será acreedor de una sanción del 1.1 % al 4 % de sus ingresos, según Art. 298 C- fracción IV.

Por lo tanto, mientras sea vigente la obligación de los concesionarios de tener una arquitectura abierta, las redes detectadas no se consideran intrusivas debido a que las computadoras y dispositivos móviles reconocerán las señales WiFi de terceros que están al alcance y expondrán la propia sin asumirlo como un acto de violación a la privacidad de la red.

Con el propósito de cubrir otros enfoques posibles, se expone la validación de los Lineamientos sobre Neutralidad en la Red, que realiza el Instituto Federal de Telecomunicaciones (IFT, 2021) en busca de garantizar un internet libre y abierto para los usua-rios con la autonomía de elegir servicios, aplicaciones y conte-nido, mediante la estandarización de algunas especificaciones técnicas de la red para una administración más homogénea por parte de los operadores.

Figura 27. Internet libre y abierto.



El fragmento puede no mantener congruencia con el tema central, pero al ser interpretado como *acceso de internet sin restricción y disponer gratuitamente de los recursos*, se ubica en una posición que accionaría en consecuencia ataques a la señal WiFi, en busca de un derecho (figura 27).

Para contrarrestar esa postura, la declaración en su contexto general se enfoca en la libertad de expresión en internet y en la disposición del recurso, con el acatamiento de tarifas y restricciones del uso en modo gratuito, señalados en las cláusulas del contrato de voluntades entre la concesionaria y usuario.

Ante los diversos escenarios expuestos, se realizan las siguientes recomendaciones para promover la protección a nivel usuario, entre el ser y el deber ser del derecho digital (ver tabla 14).

Tabla 14. Protección de red nivel usuario.

Encriptación	Escaneo	Supervisión	Ataque dirigido
Reforzar la seguridad del módem con el método de encriptación WPA2 (Wireless Protected Access), para proteger la visibilidad de la red a nivel usuario.	Programas de escaneo de la red, con la finalidad de detectar cuáles son los dispositivos que se encuentran conectados y en el caso de que exista alguno sin aprobación de origen, eliminar la conexión: Wireless Network Watcher, SoftPerfect WiFi Guard, Advanced Port Scanner, Angry IP Scanner, TP-Link Tether, Fing, entre otros.	Herramientas de auditoría wireless y hackeo ético, para monitorear la red y detectar los puntos vulnerables en el sistema de control y seguridad: Inspector Wi-Fi, Aircrack, Caín&Abel, Kismet, AirSnort, NetStumbler, Airjack, inSSiDer, WPS WPA Tester, WIFI Pass Key, WepAttack (Linux), entre otras.	Pruebas de penetración (pen test) autodirigidas, para atacar con fuerza bruta el sistema de seguridad y medir su eficacia con Kali Linux.

Finalmente, el acceso de internet tiene una posición vulnerable de alto riesgo con amenaza latente, que depende de nosotros activar los mecanismos de seguridad correspondientes para reducir la probabilidad de un ataque.

Si bien es cierto que el robo de la señal wifi puede limitarse solamente para uso particular de internet del intruso, también puede ser usado para fines no lícitos que comprometan la IP del usuario, en fraudes electrónicos.

Caso 2. ¿Invertir en plataformas digitales garantiza la seguridad del patrimonio?

Reflexión

Las plataformas digitales de inversión han incrementado significativamente su presencia en los últimos años, ofreciendo acceso a mercados financieros, criptomonedas y otros activos virtuales desde cualquier dispositivo con conexión a internet. En este contexto, es común encontrar publicidad que promete altos rendimientos, procesos de inversión simplificados y asesoría personalizada mediante plataformas de trading. Ante este escenario, surge la siguiente pregunta: ¿la existencia de una plataforma digital garantiza que el patrimonio del inversionista se encuentra protegido?[1]

El mercado digital en materia financiera crece a la par de las innovaciones tecnológicas, evolucionando los activos y los modelos de inversión; esto permite abatir los esquemas selectivos y permite mayor cobertura de participación a toda aquella persona que desee invertir su capital en acciones o divisas que cotizan en la Bolsa en plataformas de compra y venta (*trading*), con el apoyo automatizado de un intermediario digital conocido como *bróker.*

Actualmente, con el registro de nuevos usuarios, se ha identificado a dos tipos de participantes, que se perfilan según el tiempo de retorno deseado o la frecuencia de transacciones que realizan; por ejemplo, el inversionista busca beneficios a mediano

1 *Para responder esta pregunta es necesario comprender el funcionamiento de las plataformas de inversión digital, los mecanismos de seguridad que implementan y el marco normativo que regula sus operaciones.

o largo plazo, mientras que los *traders* tiene intereses de rentabilidad inmediata que les exige mayor interacción en plataforma.

La selección de una plataforma depende de su posicionamiento, el cual se obtiene a través del desempeño de los brókeres y del cumplimiento de las regulaciones previstas por la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), Comisión Nacional de Seguros y Fianzas (CNSF), Comisión Nacional Bancaria y de Valores (CNBV) y Comisión Nacional del Sistema de Ahorro para el Retiro (CONSAR), acordes a las normativas vigentes de la Ley Fintech.

Asimismo, los representantes procuran avalar la confiabilidad y seguridad de los procesos, con las Licencias CySEC (Cyprus Securities and Exchange Commission), FCA (Financial Conduct Authority), ASIC (Austrlian Securities and Investments Commission), y otras, otorgadas por los consejos de vigilancia, lo que beneficia las operaciones de control de interno de los contratos de rentabilidad por diferencia (CFD), parámetros de inversión máxima y mínima, frecuencia de pagos, demostración gratuita, accesibilidad y manejo de cuenta y garantía de protección de los datos. Aunque la lista puede ser volátil, por el alto nivel de competitividad, se citan tres opciones: *Invesa Capital, Markets.com y Capital.com*

Pero el éxito de una plataforma trading va más allá de un diseño funcional; requiere también el conocimiento sobre la Ley para Regular las Instituciones de Tecnología Financier a (LRITF, 2021), con el propósito de establecer las bases; aunque el extenso implica disposiciones para la organización, operación y funcionamiento en general.

A continuación, se citan algunos artículos que fortalecen la comprensión desde un punto de vista informático.

- Título II, Capítulo II. De las Instituciones de Fondos de Pagos Electrónicos, artículo 22 fracción III y IV; y artículo 29 fracción VI (ver figura 28).

Figura 28. Instituciones de Fondos de Pago Electrónico.



- Capítulo III. De las operaciones con Activos Virtuales, artículo 30 con la descripción de activo virtual y la relación de autoridad del Banco de México, y artículo 34 con los riesgos inherentes en el uso y manejo de dichos activos (ver figura 29).

Figura 29. De las operaciones con activos virtuales



- Título III, Capítulo II. De la Operación de las ITF, artículo 47 para el control de transacciones y artículo 56 sobre la autorización del uso de tecnologías de información, redes de comunicación y medios de autenticación (ver figura 30).

Figura 30. De la operación de las ITF.



- Capítulo III. De la Suspensión y la Revocación de la Autorización para operar como ITF, artículo 68, fracción I, por infraestructura o controles no adecuados.

Dentro de este ecosistema financiero digital, uno de los elementos que ha adquirido mayor relevancia corresponde a los activos virtuales, particularmente las criptomonedas, debido a su creciente utilización como medio de intercambio y de inversión. La criptomoneda se convierte en la unidad de valor binario que define la gestión de las transacciones que giran a su alrededor para llevar a cabo el pago de productos y servicios en un ambiente virtual; a nivel de programación se sustenta en técnicas criptográficas desarrolladas sobre la tecnología *blockchain*, mediante un esquema de seguridad de punto a punto que, a diferencia de los tokens, solo puede representar una moneda, como es el caso de Bitcoin.

La administración del sitio web, aplicaciones y sistemas de bases de datos distribuidas y/o descentralizadas, se vuelven un reto junto con la confirmación de transacciones por bloques *blockchain* o retroacción de envíos de bitcoins, para cumplir con un modelo de negocio basado en gestión estratégica. Sin embargo, la complejidad de las operaciones y la robustez en los procesos no la eximen de amenazas en busca de encontrar una vulnerabilidad que permita un ataque con beneficio económico.

Como ejemplo de mitigación de riesgos en plataformas digitales, PayPal implementa un conjunto de medidas avanzadas de seguridad que protegen tanto a compradores como a vendedores (ver figura 31). Entre ellas destacan: cifrado Secure Socket Layer (SSL) para garantizar la confidencialidad de la información durante el envío y recepción de los datos; autenticación multifactor (MFA) para verificar la identidad legal de los usuarios por medio de dispositivos vinculados; algoritmos antifraude con detección en tiempo real que monitorean las peticiones sospechosas con el propósito de verificarlas para una posterior autorización o denegación del servicio; y un programa de garantía que asegura la cobertura de pagos legítimos en caso de disputas.

Figura 31. Técnicas de seguridad.



Estas estrategias forman parte de las buenas prácticas para la protección de los activos digitales y refuerzan la confianza en las plataformas de pago frente a los recurrentes ciberataques y pérdidas económicas. Con el deber de proteger el patrimonio de los clientes de las ITF, así como, de las sociedades autorizadas de operar con modelos novedosos, se citan los delitos señalados en el artículo 132 y 133 de la Ley para Regular las Instituciones de Tecnología Financier a (LRITF, 2021) (ver figura 32).

Figura 32. Artículo 132 y 133 de LITF.



Aunque las autoridades financieras en México no reconozcan el bitcoin como moneda de curso legal, pero las Instituciones de Tecnología Financiera lo consideran en los modelos de negocios digitales, será una opción redituable para un ciberataque que puede ser sancionado por el Código Penal Federal como un acceso ilícito a los sistemas y equipos de informática de las instituciones del sistema financiero, a través de la violación de un protocolo de seguridad, con un pena de 6 meses a 4 años de prisión y 100 a 600 días de multa, referenciado en el Artículo 211 bis 4 (CPF, 2021c).

En consecuencia, la seguridad del patrimonio digital no depende exclusivamente de la infraestructura tecnológica implementada por las plataformas de inversión ni del cumplimiento

del marco regulatorio. También exige que el inversionista adopte una actitud crítica al verificar la legitimidad del proveedor, comprender los riesgos asociados a los activos virtuales, proteger sus credenciales de acceso y desconfiar de promesas de rentabilidad extraordinaria.

La cultura de ciberseguridad comienza cuando la confianza en la tecnología se acompaña de decisiones informadas y responsables.

Caso 3. ¿Un manual de políticas de seguridad informática es realmente necesario?

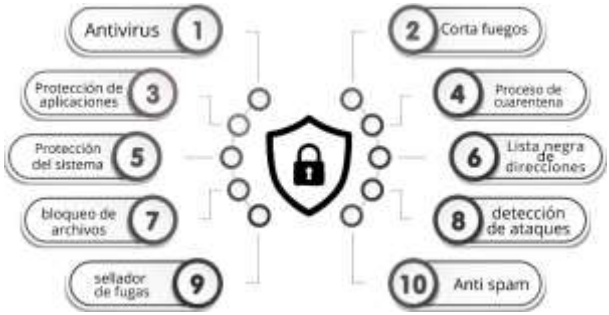
Reflexión

Una organización invierte de manera constante en equipos de cómputo, firewalls, antivirus y plataformas digitales. Sin embargo, no cuenta con políticas institucionales que regulen el uso de los recursos tecnológicos, el acceso a la información, el manejo de dispositivos externos, la utilización de plataformas de inteligencia artificial o la gestión de respaldos. Cada área opera conforme a sus propios criterios y las decisiones relacionadas con la seguridad dependen, en gran medida, de la experiencia individual de los usuarios. Ante este escenario surge la siguiente pregunta: ¿puede una organización considerarse segura únicamente por disponer de infraestructura tecnológica, aunque carezca de un manual de políticas de seguridad informática?

A primera vista podría pensarse que la seguridad informática depende principalmente de la adquisición de infraestructura tecnológica. Sin embargo, la experiencia demuestra que una parte importante de los incidentes de seguridad tiene su origen en decisiones humanas, procedimientos inexistentes o responsabilidades mal definidas. En consecuencia, la ausencia de lineamientos institucionales representa un riesgo que ninguna solución tecnológica puede eliminar por sí sola. Esta percepción suele resumirse en una expresión frecuente: «A mí no me va a pasar». Esta falsa sensación de seguridad provoca que la elaboración de políticas, la asignación de responsabilidades y la adopción de controles preventivos se pospongan hasta que ocurre un incidente.

Si observamos la situación desde una perspectiva jurídica, las organizaciones tienen la obligación de proteger la información, los datos personales y los activos digitales conforme al marco normativo aplicable. Par ello, cuentan con múltiples mecanismos de protección (ver figura 33), como antivirus, firewalls, listas de bloqueo de direcciones URL (URL Blacklist), sistemas de prevención de fuga de información (Anti-Leak), filtros de correo no deseado (Anti-Spam), aislamiento de aplicaciones (Application Guard), cuarentena de procesos (Process Quarantine), bloqueo de archivos (File Lock), protección de procesos críticos (System Guard) y mecanismos de detección de ataques (Attack Detection).

Figura 33. Mecanismos de protección.



Sin embargo, la eficacia de estos controles disminuye cuando la organización carece de políticas que regulen su implementación, administración y uso responsable. Desde la perspectiva técnica, la protección de los activos de información tampoco concluye con la implementación de controles tecnológicos. La seguridad informática requiere mecanismos permanentes de verificación que permitan conocer el nivel de protección de la organización. Entre ellos destacan tres paradigmas que se pueden ejemplificar de la siguiente manera:

- La auditoría de seguridad, orientada a evaluar la gobernanza, las políticas y el cumplimiento normativo.

Ejemplo	Acción	Resultado
Una empresa contrata una auditoría para revisar sus políticas internas, roles de acceso y cumplimiento con normas como ISO 27001.	El equipo analiza políticas internas, roles de acceso, planes de contingencia y uso de contraseñas, entre otros.	Recomendaciones estratégicas para mejorar su gobernanza de seguridad.

- La evaluación de seguridad, enfocada en identificar vulnerabilidades técnicas en sistemas, aplicaciones y dispositivos.

Ejemplo	Acción	Resultado
Un hospital realiza un análisis técnico de su red interna.	Se revisan configuraciones de firewalls, puertos abiertos y versiones de software y se identifican dispositivos conectados sin control.	El reporte revela que un servidor con un sistema operativo obsoleto es vulnerable y requiere actualización inmediata.

- Las pruebas de penetración (*pentesting*), cuyo propósito es simular ataques controlados para determinar la capacidad de respuesta de la infraestructura tecnológica; de esta manera, la tecnología contribuye a reducir vulnerabilidades.

Ejemplo	Acción	Resultado
Una fintech contrata un servicio de *pentesting* para simular un ciberataque.	El equipo logra, de forma controlada, acceder a datos sensibles usando una vulnerabilidad en una API mal configurada.	El test revela una falla en una API, que es corregida antes de que sea explotada por un atacante real.

En el ámbito de la seguridad informática, existen varios tipos de auditorías que desarrollan un proceso de revisión y evaluación sobre los controles de operación para medir el grado de seguridad y nivel de riesgo en que se encuentran los elementos sujetos a protección descritos en el manual de políticas de seguridad.

Entre ellas destacan las auditorías en informática especializadas en el área de seguridad: web, software, base de datos, redes y hardware, para detectar vulnerabilidades y amenazas (Ortega Hernández, 2014).

No existe un sistema eternamente seguro; la misma tecnología es el principal factor para perpetrar la seguridad, es por eso que la mejor estrategia son las políticas institucionales porque reducen la improvisación al establecer responsabilidades, procedimientos y criterios de actuación frente a los riesgos.

Desde el ámbito internacional, organismos especializados, como la Cybersecurity and Infrastructure Security Agency (CISA), han desarrollado guías y criterios técnicos que sirven de referencia para fortalecer la seguridad de las organizaciones. Entre las principales prácticas recomendadas se encuentran la gestión continua de vulnerabilidades mediante la actualización de sistemas y aplicaciones, el uso de mecanismos robustos de autenticación, la incorporación de configuraciones seguras desde el desarrollo del software, la realización periódica de evaluaciones de riesgo y la implementación de procesos de mejora continua, sustentados en el intercambio de información sobre incidentes y la colaboración entre los sectores público y privado. Estas recomendaciones evidencian que la ciberseguridad constituye un proceso permanente de gestión y no una acción aislada sustentada únicamente en herramientas tecnológicas.

La verificación del cumplimiento de las políticas puede apoyarse en herramientas especializadas para el inventario de activos, el monitoreo de redes, la administración de configuraciones y la detección de vulnerabilidades. Sin embargo, dichas herramientas constituyen únicamente un medio de apoyo; su eficacia depende de que la organización cuente con procedimientos, responsabilidades y criterios previamente definidos para interpretar los resultados y adoptar las acciones correctivas correspondientes.

En este contexto, un manual de políticas de seguridad informática deja de ser un documento administrativo para convertirse en un instrumento de gobernanza que establece responsabilidades, especificaciones, excepciones y procedimientos y orienta la

toma de decisiones. Su finalidad no es limitar el uso de la tecnología, sino garantizar que esta se utilice de forma segura y alineada con los objetivos institucionales.

Con el propósito de ofrecer al lector un referente metodológico para el diseño e implementación de políticas institucionales, he desarrollado una propuesta que se encuentra disponible como *Anexo 4. Manual de Políticas de Seguridad Informática*

No obstante, la implementación de un manual de esta naturaleza suele enfrentar tres desafíos institucionales. Entre los más frecuentes destacan el riesgo subestimado, el recurso subvaluado y la negligencia técnica, los cuales limitan la adopción de una cultura institucional de seguridad (ver figura 34).

- El riesgo subestimado se presenta cuando la alta dirección percibe la seguridad informática como un gasto y no como una inversión estratégica para la continuidad operativa. La falta de comprensión sobre la obligación de proteger los activos digitales y las consecuencias jurídicas, económicas y reputacionales derivadas de un incidente provoca que las políticas de seguridad carezcan del respaldo institucional necesario. Como consecuencia, se minimiza el respaldo normativo y se diluye la autoridad de las políticas de seguridad.
- El recurso subvaluado ocurre cuando la administración considera innecesario destinar recursos a la seguridad porque los sistemas aparentemente funcionan de manera adecuada. Este enfoque reactivo ignora la existencia de riesgos latentes y expone a la organización a vulnerabilidades que podrían prevenirse mediante inversiones razonables en infraestructura, capacitación y mecanismos de control. Como consecuencia, la organización queda expuesta a amenazas derivadas de decisiones económicas que desconocen el valor estratégico de un entorno digital seguro y las implicaciones que un ataque puede ocasionar sobre la infraestructura, los sistemas y las bases de datos.

- La negligencia técnica se manifiesta cuando los responsables de tecnologías de la información consideran suficiente la implementación de herramientas como firewalls, antivirus o mecanismos de cifrado, sin reconocer que la seguridad debe gestionarse de forma integral, continua y adaptativa. La ausencia de políticas, procedimientos y responsabilidades claramente definidas incrementa la probabilidad de errores humanos y limita la capacidad institucional para responder eficazmente ante un incidente.

Figura 34. Desafíos institucionales.



Como consecuencia, la organización no solo enfrenta un ataque, sino que también queda expuesta a responsabilidades derivadas de la omisión de medidas institucionales de seguridad.

La seguridad informática no se construye únicamente mediante herramientas tecnológicas; requiere liderazgo, políticas institucionales y una cultura organizacional orientada a la prevención. Un manual de políticas de seguridad informática representa el instrumento mediante el cual la organización traduce los principios jurídicos, las buenas prácticas internacionales y los controles técnicos en responsabilidades concretas, procedimientos verificables y criterios de actuación. En un entorno donde las amenazas evolucionan constantemente, normar el uso de la tecnología deja de ser una decisión administrativa para convertirse en un componente esencial de la gobernanza, la gestión del riesgo y la resiliencia institucional

REFLEXIONES

A lo largo de esta obra se ha mostrado que proteger los activos de información y fortalecer la resiliencia digital requiere articular tres dimensiones inseparables: la estrategia y la gobernanza institucional, los controles técnicos y la participación responsable de las personas.

El primer capítulo permitió reconocer que una organización ciberresiliente necesita dirigir y gestionar el riesgo desde una perspectiva estratégica, sustentada en el marco jurídico, la gobernanza, la definición de responsabilidades y la mejora continua. El segundo mostró que esta visión debe traducirse en mecanismos técnicos y operativos capaces de proteger la infraestructura y los activos digitales frente a vulnerabilidades y amenazas. El tercero permitió comprender que ninguna medida de protección puede sostenerse en el tiempo sin una cultura de seguridad que involucre a las personas y promueva prácticas responsables en el uso de la tecnología y en la protección de los datos.

Esta articulación permite comprender que la seguridad depende de la capacidad institucional para anticipar riesgos, evaluar los controles y aprender de sus resultados. La ciberseguridad debe asumirse, como un proceso permanente de prevención, adaptación y mejora, en el que la organización no busca eliminar por completo el riesgo, sino desarrollar capacidades para identificarlo, gestionarlo, responder ante los incidentes y aprender de ellos.

Los anexos e instrumentos que acompañan la obra buscan facilitar su aplicación en contextos organizacionales y formativos, favoreciendo las acciones de prevención, evaluación y mejora.

Finalmente, la ciberseguridad, es una responsabilidad permanente. Su fortaleza reside en la capacidad de las organizaciones y las personas para adaptarse, aprender y actuar responsablemente frente a un entorno digital en constante transformación.

GLOSARIO

Glosario

Taxonomía de la ciberseguridad

- *Ciberamenaza*. Riesgo potencial relacionado a las vulnerabilidades de los sistemas informáticos e infraestructura física y pasiva de las redes públicas de telecomunicaciones de permitir causar daño a los procesos y continuidad de las infraestructuras Críticas de Información, las Infraestructuras de Información Esenciales, así como la seguridad de las personas (Guerra Mena, 2022).
- *Ciberataque.* Acción realizada a través de las re-des de telecomunicaciones con el objetivo de da-ñar las Infraestructuras Críticas de Información, las Infraestructuras de Información Esenciales, así como la seguridad de las personas (Guerra Mena, 2022).
- *Ciberdefensa*. Conjunto de acciones, recursos y mecanismos del estado en materia de seguridad nacional para prevenir, identificar y neutralizar toda ciberamenaza o ciberataque que afecte a la infraestructura crítica nacional (Guerra Mena, 2022).
- *Ciberdelincuencia*. Actividades que llevan a cabo individuo(s) que utilizan como medio o como fin a las tecnologías de la información y comunicación en la comisión de delitos (Guerra Mena, 2022).

- *Ciberespacio.* Es un entorno digital global constituido por redes informáticas y de telecomunicaciones, en el que se comunican e interactúan las personas y permite el ejercicio de sus derechos y libertades como lo hacen en el mundo físico (Guerra Mena, 2022).
- *Ciberresilencia.* Capacidad de un sistema para recuperarse de un fallo y mantener la confiabilidad en el servicio (Guerra Mena, 2022).
- *Ciberriesgo*. La posibilidad de que una amenaza aproveche una vulnerabilidad y cause pérdida o daño sobre los activos de las tecnologías de información y comunicaciones (Guerra Mena, 2022).
- *Ciberseguridad.* Conjunto de políticas, controles, procedimientos, métodos de gestión de riesgos y normas asociadas con la protección de la sociedad, gobierno, economía y seguridad nacional en el ciberespacio y las redes públicas de telecomunicación (México, 2017).

Triada de la ciberseguridad

- *Confidencialidad.* Propiedad de que la información no se ponga a disposición ni se divulgue a individuos, entidades o procesos no autorizados (ISO/IEC_27000, 2026).
- *Integridad.* Propiedad de exactitud y completitud. Garantiza que el contenido permanezca consistente y confiable durante todo su ciclo de vida. (ISO/IEC_27000, 2026).
- *Disponibilidad.* Propiedad de ser accesible y utilizable bajo demanda por una entidad autorizada (ISO/IEC_27000, 2026).

Tipos de Ataques de infiltración por ingeniería social

- *Phishing*. Estafa digital mediante mensajería instantánea, redes sociales y correos electrónico para direccionar a un sitio web que solicita datos personales y sensibles, con el propósito de suplantar la identidad; se presentan otras modalidades de infiltración:

- *Qrshing*. Estafa digital mediante el código QR
- *Smishing.* Estafa digital mediante mensaje SMS
- *Vishing.* Estafa digital mediante telefonía con voz.
- *Spear phishing*. Estafa digital dirigida que tiene información personal de la víctima, dando confianza para el seguimiento de las indicaciones hasta lograr burlar los firewall o controles de seguridad, es enviada supuestamente por familiares o fuentes confiables.
- *Whaling*. Estafa digital más ambiciosa que va a la pesca de ejecutivos, el ataque es a nivel gerencial haciéndose pasar por entidades de autoridad, simulando falta legales o fiscales creando un ambiente estresante para obtener los datos sensibles a la mayor brevedad.
- *Trashing*. Estafa digital mediante la recuperación de datos en contenedores o papeleras de reciclaje digital
- *Catfish*. Estafa digital mediante la suplantación de identidad por redes sociales o aplicaciones de citas.

Tipos de Violencia

- *Violencia digital*. Comprende conductas de acoso, hostigamiento, amenazas, persecución, ciberbullying, doxing, stalking, trolling, etc. El bien jurídico principal es la dignidad, integridad, salud emocional y psicológica, identidad y libre desarrollo de la personalidad.
- *Violencia digital sexual.* Protege la libertad e indemnidad sexual, la intimidad y la autodeterminación sexual. Aquí se ubican el *grooming, sextorsión, sexting* no consentido, difusión de contenido íntimo y, muy importante, la creación mediante IA de imágenes, audios o videos sexuales simulados (*deepfakes sexuales*).
- *Violencia mediática.* No es exactamente lo mismo que violencia digital. se refiere a la difusión masiva de contenidos que promueven o reproducen violencia contra las mujeres a través de medios de comunicación o plataformas digitales.

Tipos de Malware

Malware. Es un programa malicioso de invasión, que puede ser infiltrado por correo electrónico, mensajería instantánea y redes sociales mediante el intercambio de archivos infectados, y de forma local por medios extraíbles [USB/Stick/SD] con el propósito de causar daño al sistema operativo, programas, aplicaciones y archivos digitales, incluyendo a los controladores y al disco duro. En casos más específicos, el ataque es dirigido al propietario del ordenador o cuenta, a través de la obtención ilícita de datos personales e información confidencial, localizada en los dispositivos locales e incluso en la nube (Ortega C. , 2022).

Se ofrece una clasificación con características específicas:

- *Virus.* Tienen la propiedad de polimorfismo y mutación, para no ser detectado y adaptarse al sistema anfitrión con la distinción de que requieren la intervención humana para iniciar la activación del programa malicioso, generalmente de forma involuntaria, y con el desconocimiento de la acción y consecuencia.
    - *Gusanos.* Es una variante autónoma del virus de reproducción automática, con un alto riesgo de proliferación por medios electrónicos y digitales, que se apoderan del registro de contactos del usuario para replicarse y expandirse, repitiendo sucesivamente el mismo proceso con los contactos del nuevo huésped infectado, provocando una reacción en cadena que consume los recursos de los servidores redes y WEB, interrumpiendo la comunicación con los dispositivos.

- *Troyano.* Tienen la capacidad de manipular local o remotamente los controladores, pero no pueden replicarse sin la participación humana; su acceso y activación se logra mediante la manipulación o engaño del usuario (ingeniería social), permitiendo de forma inmediata extraer las contraseñas de todas las cuentas resguardadas, exponiendo los datos personales e información confidencial, y dejando a disposición los controladores del sistema,

dispositivos, red e Internet, que pueden ser activados a merced del delincuente y acceder a la privacidad del individuo sin restricciones. Por ejemplo: las webcams que capturan y envían las imágenes por internet, pueden ser activadas de manera remota y obtener información ilícitamente; lo mismo aplica a las cámaras de video vigilancia y todos los sistemas audiovisuales que requieran una IP y cuenta electrónica del usuario.

- *Spyware:* Es un espía que se infiltra mediante exploits, troyanos, enlaces, o con un USB de forma local en el ordenador, tabletas y celulares, y se oculta para no ser descubierto, con el propósito de registrar toda información confidencial y el histórico de navegación de las víctimas, y además enviarlo remotamente al atacante. A continuación, una clasificación más específica:
  - *Keylogger o infostealers*: Es una variante que registra todas las pulsaciones realizadas en el teclado, dejando al descubierto los que se escribe durante una sesión activa: nombres de usuarios, contraseñas, mensajes en aplicaciones de redes sociales, incluyendo la información de correos electrónicos y plataformas digitales.
  - *Stalkerware o Spouseware:* Aplicación móvil de vigilancia profunda de control parental o de acecho a la pareja, con el reporte en tiempo real de la ubicación, mensajes, llamadas, notificaciones, fotos, videos y más. Instalado localmente en el dispositivo.
  - *Red Shell:* Espía preinstalado en los juegos en línea por los propios desarrolladores, para rastrear la actividad de los usuarios durante las sesiones, incluyendo la navegación a sitios, páginas y plataformas, y los datos de acceso. Algunos de los juegos se encuentran en la plataforma Steam, que distribuye contenido de entretenimiento.
  - *Cookies,* programa de rastreo que registra los historiales de navegación web y credenciales de autenticación, para recordar los accesos y crear perfiles de usuario, no se requiere de infiltración porque se encuentra en las

prestaciones de los servicios web; sin embargo, contiene un fichero de dato codiciado por los atacantes.

- *Adware:* Combina el espionaje con el ataque de publicidad no solicitada (SPAM), entre las formas más comunes de infiltrarse a nuestros dispositivos se encuentran: la precarga de aplicaciones por los fabricantes, descarga no autorizada de archivos en sitios web infectados, y descarga de aplicaciones gratuitas y libres. Una vez alojados inician con el rastreo de las pulsaciones del teclado para obtener del historial Web el registro de navegación con las páginas más frecuentes, permitiendo identificar el perfil del usuario y facilitar la publicidad dirigida con carga de anuncios no esperados.

  También es una estrategia de publicidad invasiva que accede a las cuentas de usuario; en donde lamentablemente el cambio de navegador como medida de protección no exime de su reiterada ejecución. En el caso de las plataformas streaming oficiales que distribuyen contenido audiovisual en su versión gratuita presentan la opción de <omitir anuncio>, obviamente no se trata de Adware, pero se sugiere extremar precauciones en los anuncios en línea de fuentes sospechosas que dirigen a sitios fraudulentos y con la tenacidad de descargar archivos sin autorización. A continuación, algunas variantes:

  - *Junkware:* Son preinstalados en los dispositivos electrónicos por el fabricante que registran los datos del usuario al iniciar el servicio y el perfil de navegación, para mostrar los anuncios de los desarrolladores, también se le conoce como *crapware o bloatware.*
  - *Freeware y Shareware.* Se pueden descargar gratuita y libremente (no confundir con *Open Source*), la primera ofrece prestaciones, sin la oportunidad de acceder al código para realizar actualizaciones o adecuaciones y la segunda, le suma la restricción de tiempo de prueba, para motivar al usuario a comprar el producto y en el inter presentar anuncios publicitarios.

  - *Pornware.* Con contenido para adultos, que instalan sin autorización programas que presentan anuncios publicitarios y dirigen a sitios web con servicios de pornografía.

- *Ransoware.* Programa secuestrador del sistema que impide el acceso a de los usuarios propietarios a sus archivos a cambio de un rescate financiero, mediante el pago digital a tarjetas de regalo, crédito o plataformas de bitcoin. Se infiltra por medios de comunicación electrónica y digital, empleando enlaces a sitios fraudulento o descarga de archivos anexos, obligando a la víctima a participar bajo amenaza de extorsión y manipulación. Entre las principales cepas se encuentran:
  - *Scareware.* Extorsión en base al engaño sobre la actualización de los servicios tecnológicos por una supuesta agencia de TI, que brinda protección a los archivos en riesgo a cambio de una cuota de recuperación.
  - *Lockware.* Extorsión en base a la intimidación por una supuesta agencia de ciberseguridad o policía cibernética, para liberar el bloqueo de la pantalla activado en consecuencia del rastreo de una actividad ilícita a cambio de una multa correspondiente a la sanción.
  - *Encrypware.* Extorsión en base al engaño e intimidación, por el cifrado de datos negando el acceso a los archivos a cambio de un rescate, si la empresa tiene el respaldo de la base de datos y activa el protocolo de recuperación, no requiere someterse a la voluntad de los delincuentes

Tipos de especialista en ciberseguridad

- *Hacker.* Especialista en ciberseguridad, también conocido como hacker de *sombrero blanco (white hat),* que realiza pruebas penetración y evaluación de vulnerabilidades en sistemas, sitios web, aplicaciones y bases de datos, con el propósito de fortalecer su seguridad.

- *Cracker.* Especialista también conocido como hacker de *sombrero negro (black hat)* que viola la seguridad de un sistema informático con fines ilícitos. Sus técnicas de ataque evolucionan constantemente para evadir las nuevas medidas de seguridad.

Entre el blanco y negro se derivan:

  - *Hacker de sombrero gris.* Operan en un limbo ético. Encuentran fallos sin permiso y, a veces, los exponen públicamente o piden recompensa por arreglarlos.
  - *Hacker de sombrero rojo.* Actúan como justicieros. Su objetivo es neutralizar a los hackers de sombrero negro destruyendo sus servidores o herramientas.
  - *Hacker de sombrero azul.* Profesionales de seguridad externos (como los invitados por Microsoft) contratados para encontrar fallos antes del lanzamiento de un producto.
  - *Hacker de sombrero verde.* Principiantes sin conocimientos avanzados, pero muy motivados por aprender técnicas de hacking y entender cómo funcionan los ataques.

- *Phreaker.* Especialista que dirige sus ataques a sistemas de telefonía, redes de telecomunicaciones y dispositivos móviles para explotar sus vulnerabilidades.
- *Defacer.* Especialista que realiza un ataque de desfiguración web, cambiando el aspecto visual de un sitio.
- *Script Kiddie.* Especialista principiante en ciberseguridad que aplica programas, scripts o exploits creados por terceros para llevar a cabo ataques o intrusiones, sin conocer realmente la estructura lógica del código que ejecutan.
- *Lamer.* Es un individuo inexperto que presume ser especialista en ciberseguridad, con conocimiento erróneo o nulo que degrada el trabajo de los programadores reales.

Términos de Seguridad Informática

- *Autenticación.* Proceso mediante el cual se verifica la identidad de un usuario, sistema o dispositivo, generalmente mediante contraseñas, tokens o biometría.
- *Derecho Digital.* Son las garantías que protegen las libertades y la privacidad de las personas en el entorno digital. Estos derechos aseguran que cada usuario de internet pueda acceder, utilizar y comunicarse en línea sin temor a violaciones de privacidad o restricciones indebidas a su libertad de expresión. Son fundamentales para una participación segura y libre en la sociedad digital (UNIR, s.f.).
- *Pentesting.* Es un ciberataque simulado y legal en el que un experto (pentester) busca vulnerabilidades en redes, software o servidores. Su propósito principal es encontrar y solucionar fallos de seguridad críticos antes de que los delincuentes puedan explotarlos, protegiendo así los datos sensibles de la organización (IBM, s.f.). Tipos de pruebas:
  - *Pentest de aplicaciones*. Enfocado en aplicaciones y sistemas relacionados, incluidas aplicaciones web y sitios web, aplicaciones móviles y de IoT.
  - *Pentest de la red*. Las pruebas son externas e internas, la primera para detectar problemas de seguridad en activos orientados a Internet, como servidores, enrutadores, sitios web y ordenadores de empleados y la segunda para descubrir vulnerabilidades que una persona podría explotar desde dentro de la red, por ejemplo, abusando de los privilegios de acceso para robar datos confidenciales.

- *Riskware*. Son aplicaciones legítimas con la capacidad de realizar funciones administrativas, de acceso remoto, monitoreo o gestión del sistema que compromete la seguridad informática. Por sus características, se convierten en herramientas de acceso remoto, clientes de administración de redes, utilidades FTP, servidores proxy y programas que modifican configuraciones de seguridad

del sistema. Se recomiendan controlar estrictamente la instalación de este tipo de software, verificar su procedencia, mantenerlo actualizado y eliminar aquellas aplicaciones que no sean indispensables para la operación del equipo (Kaspersky, s.f.).

Términos sobre tecnologías de información y comunicaciones.

- *Base datos.* Es un repositorio organizado de información o datos, diseñado para almacenar, administrar y recuperar información de manera eficiente, facilitando su consulta, actualización y procesamiento mediante un sistema de gestión de bases de datos (DBMS) (NIST, s.f.).
- Dispositivo externo. Cualquier equipo de almacenamiento portátil como USB, discos duros externos, tarjetas SD, etc.
- Firewall. es un mecanismo de seguridad de hardware, software o una combinación de ambos que supervisa y controla el tráfico de red entrante y saliente con base en un conjunto de reglas predefinidas, con el propósito de impedir accesos no autorizados y proteger los sistemas y redes informáticas (NIST-a,2009).
- Hardware. corresponde al conjunto de componentes físicos y tangibles de un sistema informático, tales como el procesador, memoria, dispositivos de almacenamiento, periféricos y equipos de comunicación, que permiten la ejecución del software y el procesamiento de datos (NIST, s.f.).
- Plataformas digitales. es un entorno tecnológico integrado por hardware, sistema operativo y otros componentes de software que proporciona la infraestructura necesaria para ejecutar aplicaciones, ofrecer servicios digitales y facilitar la interacción entre usuarios, procesos y recursos informáticos (NIST, s.f.).
- Respaldo (backup). Copia de seguridad de información crítica, almacenada de forma segura para ser recuperada en caso de pérdida o falla.

- Sitio WEB. es un conjunto estructurado de páginas y recursos digitales relacionados entre sí, accesibles mediante una dirección web (URL) a través de Internet y publicados bajo un mismo dominio, con el propósito de ofrecer información, servicios o interacción con los usuarios. Esta definición es consistente con la arquitectura y los principios establecidos por el World Wide Web Consortium (W3C) (NIST, s.f.).
- Software. es el conjunto de programas, procedimientos, instrucciones y datos asociados que permiten a un sistema informático ejecutar tareas específicas y controlar el funcionamiento del hardware. Comprende tanto los sistemas operativos como las aplicaciones y demás componentes lógicos necesarios para el procesamiento de la información (NIST, s.f.).

Referencias

I. Legislación y normativa nacional

Código de Comercio, CC. (2024). *Código de Comercio*. DOF, 30 de diciembre de 2024. https://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo38904.pdf

Código Civil Federal, CCF. (2024). *Código Civil Federal*. DOF, 17 de enero de 2024. https://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo17186.pdf

Código Penal Federal, CPF. (2026). *Código Penal Federal: Revelación de secretos y acceso ilícito a sistemas y equipos de informática*. DOF, 13 de marzo de 2026. https://www.diputados.gob.mx/LeyesBiblio/pdf/CPF.pdf

Constitución Política de los Estados Unidos Mexicanos, CPEUM. (2026). *Constitución Política de los Estados Unidos Mexicanos*. DOF, 10 de abril de 2026. https://transparencia-ciudadana.scjn.gob.mx/sites/default/files/page/2026-04/cpeum10042026.pdf

Ley de Aviación Civil, LAC. (2023). *Ley de Aviación Civil.* DOF, 3 de mayo de 2023. https://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo83106.pdf

Ley de Firma Electrónica Avanzada, LFEA. (2021). *Ley de Firma Electrónica Avanzada.* DOF, 20 de mayo de 2021. https://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo67194.pdf

Ley de Instituciones de Crédito, LIC. (2024). *Ley de Instituciones de Crédito*. DOF, 24 de enero de 2024. https://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo12.pdf

Ley Federal de Protección al Consumidor, LFPC. (2023). *Ley Federal de Protección al Consumidor*. DOF, 21 de diciembre de 2023.

Ley Federal de Protección a la Propiedad Industrial, LFPPI. (2020). *Ley Federal de Protección a la Propiedad Industrial.* DOF, 1 de julio de 2020. https://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo122873.pdf

Ley Federal de Protección de Datos Personales en Posesión de los Particulares, LFPDPPP. (2025). *Ley Federal de Protección de Datos Personales en Posesión de los Particulares.* DOF, 14 de noviembre de 2025. https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Ley Federal de Telecomunicaciones y Radiodifusión, LFTR. (2024). *Ley Federal de Telecomunicaciones y Radiodifusión*. DOF, 1 de abril de 2024. https://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo97329.pdf

Ley Federal del Derecho de Autor, LFDA. (2020). *Ley Federal del Derecho de Autor*. DOF, 1 de julio de 2020. https://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo17068.pdf

Ley Federal del Trabajo, LFT. (2025). *Ley Federal del Trabajo*. DOF, 21 de febrero de 2025. https://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo125151.pdf

Ley Federal de Transparencia y Acceso a la Información Pública, LFTAIP. (2024). *Ley Federal de Transparencia y Acceso a la Información Pública.* DOF, 1 de abril de 2024. https://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo112906.pdf

Ley General de Acceso de las Mujeres a una Vida Libre de Violencia, LGAMVLV. (2024). *Ley General de Acceso de las Mujeres a una Vida Libre de Violencia*. DOF, 26 de enero de 2024. https://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo17079.pdf

Ley General de Archivos, LGA. (2018). *Ley General de Archivos.* DOF, 19 de enero de 2023. https://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo120902.pdf

Ley General de Educación, LGE. (2019). *Ley General de Educación.* Diario Oficial de la Federación. DOF, 30 de septiembre de 2019. https://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo124435.pdf

Ley General de Educación Superior, LGES. (2021). *Ley General de Educación Superior*. DOF, 20 de abril de 2021. https://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo124400.pdf

Ley General de Inclusión de las Personas con Discapacidad, LGIPD. (2024). *Ley General para la Inclusión de las Personas con Discapacidad*. DOF, 14 de junio de 2024. https://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo61725.pdf

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, LGPDPPSO. (2025). *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.* DOF, 20 de marzo de 2025. https://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo125096.pdf

Ley General de Transparencia y Acceso a la Información Pública, LGTAIP. (2025). *Ley General de Transparencia y Acceso a la Información Pública*. DOF, 20 de marzo de 2025. https://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo125097.pdf

Ley General del Sistema Nacional de Seguridad Pública, LGSNSP. (2024). *Ley General del Sistema Nacional de Seguridad Pública*. DOF, 16 de diciembre de 2024. https://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo96855.pdf

Ley General de Títulos y Operaciones de Crédito, LGTOC. (2024). *Ley General de Títulos y Operaciones de Crédito*. DOF, 26 de marzo de 2024. https://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo42.pdf

Ley General en Materia de Humanidades, Ciencias, Tecnologías e Innovación, LGHCTI. (2023). *Ley General en materia de Humanidades, Ciencias, Tecnologías e Innovación*. DOF, 8 de mayo de 2023. https://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo124801.pdf

Ley de Protección y Defensa al Usuario de Servicios Financieros, LPDUSF. (2024). *Ley de Protección y Defensa al Usuario de Servicios Financieros*. DOF, 24 de enero de 2024. https://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo18.pdf

Ley para Regular las Instituciones de Tecnología Financiera, LRITF. (2024). *Ley para Regular las Instituciones de Tecnología Financiera*. DOF, 24 de enero de 2024. https://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo120920.pdf

II. Normativa, estándares y organismos internacionales

Consejo de Derechos Humanos, CDH. (2018). *Promoción y protección de todos los derechos humanos, civiles, políticos, económicos, sociales y culturales, incluido el derecho al desarrollo*. Naciones Unidas. https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_38_L10.pdf

Digital Markets Act, DMA. (s. f.). *Ley de Mercados Digitales*. https://digital-markets-act.ec.europa.eu/index_en

Digital Services Act. DSA. (s. f.). *Ley de Servicios Digitales*. https://www.eu-digital-services-act.com/Digital_Services_Act_Articles.html

International Organization for Standardization, ISO/IEC_27001. (2022). *Information security, cybersecurity and privacy protection—Information security management systems—Requirements*. https://www.iso.org/es/norma/27001

International Organization for Standardization, ISO/IEC 27000. (2026). *Information security, cybersecurity and privacy protection—Information security management systems*. https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-6:v1:en

International Organization for Standardization ISO_27001:27002. (s.f.). *Guía para iplementar ISO 27001 paso a paso*. https://www.normaiso27001.es/fase-2-analisis-del-contexto-de-la-organizacion-y-determinacion-del-alcance/

National Institute of Standards and Technology, NIST. (s. f.). *Information Technology Laboratory Computer Security Resource Center*. https://csrc.nist.gov/glossary/term/software

National Institute of Standards and Technology, NIST-a. (2009). *Guidelines on firewalls and firewall policy*. Special Publication 800-41 Rev. 1. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

National Institute of Standards and Technology, NIST-b. (2026). *El NIST actualiza sus operaciones de NVD para abordar el crecimiento récord de CVE.* https://www.nist.gov/news-events/news/2026/04/nist-updates-nvd-operations-address-record-cve-growth

National Institute of Standards and Technology, NIST-C. (2026).

El NIST rediseña la Base de Datos de Vulnerabilidades para la era de la IA: lo que las organizaciones deben entender. https://www.intedya.com/internacional/5109/noticia-el-nist-redisena-la-base-de-datos-de-vulnerabilidades-para-la-era-de-la-ia-lo-que-las-organizaciones-deben-entender.html

The Institute of Internal Auditors, IIA. (2026). *Requisito temático de ciberseguridad (Topical Requirement).* https://www.theiia.org/globalassets/site/standards/topical-requirements/cybersecurity/cybersecurity_topical_requirement_spanish.pdf

III. Documentos legislativos e iniciativas

Corona Nakamura, M. D. (2022). *Reforma a Ley de Seguridad Nacional*. Documento legislativo, 3 de agosto de 2022. https://infosen.senado.gob.mx/sgsp/gaceta/65/1/2022-08-03-1/assets/documentos/Inic_PVEM_Dip_Nakamura_art_5_LSN.pdf

Elizon Guerra, O. J. (2026). *Reforma a Ley de Seguridad Nacional*. Documento legislativo, 7 de abril de 2026. https://sil.gobernacion.gob.mx/Archivos/Documentos/2026/04/asun_5073240_20260421_1775655999.pdf

Guerra Mena, J. (2022). *Ley General de Ciberseguridad*. Documento legislativo, 03 de octubre de 2022. https://sil.gobernacion.gob.mx/Archivos/Documentos/2022/12/asun_4475036_20221215_1665067316.pdf

Hernández Pérez, M. E. (2022). *Reforma a la Ley de Seguridad Nacional*.Documentolegislativo,11deoctubrede2022.https://sil.gobernacion.gob.mx/Archivos/Documentos/2022/12/asun_4465436_20221208_1665511763.pdf

López Casarín, J. J. (2024). *Ley Federal de Ciberseguridad*. Documento legislativo, 20 de marzo de 2024. https://gaceta.diputados.gob.mx/PDF/65/2024/mar/20240320-II-4-1.pdf

Mancera Espinosa, M. A. (2020). *Ley General de Ciberseguridad.* Documento legislativo, 1 de septiembre de 2020. https://sil.gobernacion.gob.mx/Archivos/Documentos/2020/09/asun_4064516_20200902_1599062884.pdf

Pinedo Alonso, C. C. (2022). *Reforma Ley de Seguridad Nacional*. Documento legislativo, 7 de diciembre de 2022.

https://sil.gobernacion.gob.mx/Archivos/Documentos/2024/05/asun_4758117_20240522_1716410903.pdf

Soto Ruíz, A. L. (2024). *Ley Federal de Ciberseguridad y Confianza Digital*. Documento legislativo. https://infosen.senado.gob.mx/sgsp/gaceta/65/3/2024-08-14-1/assets/documentos/Inic_GPPVEM_Sen_Lagunes_ley_Fed_Ciberseguridad.pdf

Trasviña Waldenrath, J. L. (2024). *Ley General de Ciberseguridad Ciudadana*. Documento legislativo, 10 de diciembre de 2024. https://sil.gobernacion.gob.mx/Archivos/Documentos/2024/12/asun_4825644_20241213_1733857236.pdf

Von Roehrich de la Isla, C. D. (2020). *Iniciativa de Ley de Ciberseguridad para la Ciudad de México*. Documento legislativo, 27 de octubre de 2020. https://56bb-87fb-8293-49f1-a1c4-8aee0b9b7151.usrfiles.com/ugd/682222_cf7448286baa4e4baee5e93c8cc7524f.pdf

IV. Artículos científicos

Arroyabe, MF, Arranz, CFA, De Arroyabe, IF, & Fernandez de Arroyabe, JC (2026). *Navegando por la ciberseguridad: el impacto del entorno en la adopción de estándares y la participación del consejo directivo.* https://doi.org/10.1080/08874417.2024.2394440

Chaudhuri, A., Kumar Behera, R., & Kumar Bala, P. (2025). *Factors impacting cybersecurity transformation: An Industry 5.0 perspective.* https://www.sciencedirect.com/science/article/abs/pii/S016740482400573X?via%3Dihub

Ghafoori, A., Gupta, M., Merhi, M., Gupta, S. (2024). *Hacia el papel de la cultura organizacional en la transformación digital basada en datos*. https://doi.org/10.1016/j.ijpe.2024.109205

Handri, E. Y., Sensuse, D. I., & Lusa, S. (2024). *Examining cybersecurity culture: Trends and success factors*. https://doi.org/10.58346/JISIS.2024.I3.020

Iqbal, A., Khan U.S., Niazi, M., Humayun, M., Sama, U.N., Khan, A.A. (2023). *Advancing database security: A comprehensive systematic mapping study of potential challenges*. https://doi.org/10.1007/s11276-023-03436-z

Ivanov, D. (2022). *El marco de la Industria 5.0: integración basada en la viabilidad de las perspectivas de resiliencia, sostenibilidad y enfoque centrado en el ser humano International*. https://doi.org/10.1080/00207543.2022.2118892

Jacome, M. G. (2026). Gobernanza de la seguridad corporativa en la era digital: Desafíos estratégicos y ciberamenazas en Colombia y América Latina. https://doi.org/10.46661/respublica.13640

Salem, A. H., Azzam, S.M, Emam, O.E., Abohany, A.A. (2024). Advancing cybersecurity: A comprehensive review of AI-driven detection techniques. https://doi.org/10.1186/s40537-024-00957-y

Umaña, G. E., & Turcio Alvarenga, M. (2024). Institucionalidad regional frente a la Cuarta Revolución Industrial: Transición hacia una gobernanza digital. *[Revista por verificar]*. https://doi.org/10.32418/rfs.2024.309.5347

V. Libros y publicaciones académicas

Caballero Velasco, M. Á., & Cilleros Serrano, D. (2022). *El libro del Hacker*. Anaya Multimedia. ISBN 978-84-415-4433-8 https://anayamultimedia.es/libro/titulos-especiales/el-libro-del-hacker-edicion-2022-maria-angeles-caballero-velasco-9788441544338/

Mitnick, K. D. (2002). *The art of deception: Controlling the human element of security*. Wiley. ISBN 978-0-471-23712-9.

Ortega Hernández, C. C. (2014). *Auditoría informática asistida por tecnología con dictamen y sugerencias*. Universidad Autónoma de Chiapas. ISBN 9786078304. https://repositorio.unach.mx/jspui/handle/123456789/3818

Ortega, C. C., Velasco, L., & López, N. (2023). *La legislación informática y el derecho digital en la formación tecnológica del profesionista*. CONAIC. ISBN 978-607-59333-1-3 https://www.conaic.net/publicaciones/Libro%20CONAEVAL%202023.pdf

Quadra-Salcedo, T., & Piñar Mañas, J. L. (2018). *Sociedad Digital y Derecho. Madrid*. ISBN 978843402483

Schneier, B. (2011). *Secrets and lies: Digital security in a networked world*. ISBN 978-1-118-08227-0

VI. Fuentes técnicas y profesionales

Conrad, K. (2024). *Tipos de ataques de inyección SQL*. Oneleet.

https://www.oneleet.com/blog/what-are-sql-injections-and-how-to-prevent-them-copy

IBM. (s. f.). *¿Qué es el pentesting?* https://www.ibm.com/mx-es/think/topics/penetration-testing

Invicti. (2026). *Secuencias de comandos entre sitios (XSS)*. https://www.invicti.com/platform-overview

Kaspersky. (s. f.). *What is Riskware?* https://www.kaspersky.com/resource-center/threats/riskware

Mozilla Developer Network, MDN. (s. f.). *Inyección SQL*. https://developer.mozilla.org/en-US/docs/Glossary/SQL_Injection

NQA. (2025). *Guía de implementación de sistemas de gestión de seguridad de la información: ISO 27001:2022*. https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

Oracle México. (2025). *¿Qué es un firewall de aplicaciones web (WAF)?* Oracle Cloud Infrastructure. https://www.oracle.com/mx/security/cloud-security/what-is-waf/

Singh, S., & Yesil, K. (2026). *Analizando los 5 ataques de inyección SQL más comunes*. Pentest-Tools. https://pentest-tools.com/blog/sql-injection-attacks

VII. Fuentes institucionales y de divulgación

Carta de Derechos Humanos y Principios para Internet, CDHPI. (2015). https://www.palermo.edu/cele/pdf/Carta-de-Derechos-Humanos-y-Principios-para-Internet-en-Espanol.pdf

Centro de Estudios de Internet y Sociedad. (2015). *Carta de Derechos Humanos y Principios para Internet*. https://www.palermo.edu/cele/pdf/Carta-de-Derechos-Humanos-y-Principios-para-Internet-en-Espanol.pdf

Coordinación de Estrategia Digital Nacional, CEDN. (2021). *Acuerdo por el que se emiten disposiciones para impulsar el uso de la informática, el gobierno digital, las TIC y la seguridad de la información*. DOF, 6 de septiembre de 2021. https://www.gob.mx/cms/uploads/attachment/file/678862/ACUERDO_Por_El_Que_Se_Emiten_Las_Pol_ticas_Y_Disposiciones_Para_Impulsar_El_Uso_Y_Aprovechamiento.pdf

Dirección General de Aeronáutica Civil, DGAC. (2017). *Circular obligatoria CO AV-23/10 R4*. https://www.gob.mx/cms/uploads/attachment/file/603112/co-av-23-10-r4_.pdf

Guardia Nacional. (2025). *Guardia Nacional recibe declaración de cumplimiento del CERT-MX bajo el Modelo SIM3 CSIRTAmericas Baseline*. Gabinete de Seguridad, Gobierno de México. https://gabinetedeseguridad.gob.mx/contenido/6650/guardia-nacional-recibe-declaracion-de-cumplimiento-del-cert-mx-bajo-el-modelo-sim3-csirtamericas-baseline

Gobierno de México. (2017). *Estrategia Nacional de Ciberseguridad*. https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

Secretaría Anticorrupción y Buen Gobierno. (2025). *Buen Gobierno investiga posible incidente de seguridad en bases de datos personales en posesión de instituciones públicas*. Gobierno de México. https://www.gob.mx/buengobierno/prensa/buen-gobierno-investiga-posible-incidente-de-seguridad-en-bases-de-datos-personales-en-posesion-de-instituciones-publicas

Ley Ingrid, LI. (s. f.). *Ley Ingrid*. Orden Jurídico. https://ordenjuridico.gob.mx/violenciagenero/LEY%20INGRID.pdf

Ley Olimpia, LO. (s. f.). *Ley Olimpia*. Orden Jurídico. https://ordenjuridico.gob.mx/violenciagenero/LEY%20OLIMPIA.pdf

Organización de los Estados Americanos, OEA. (2019). *Estado de la ciberseguridad en el sistema financiero mexicano*. Secretaría General de la Organización de los Estados Americanos. https://www.oas.org/es/sms/cicte/documents/informes/Estado-de-la-Ciberseguridad-en-el-Sistema-Financiero-Mexicano.pdf

Ortega, C. (2022). *Malware, la mayor amenaza para una sociedad basada en el conocimiento digital*. https://www.orcamx.mx/post/malware-la-mayor-amenaza-para-una-sociedad-basada-en-el-conocimiento-digital

UNIR. (s. f.). *¿Qué son los derechos digitales?* Universidad Internacional de La Rioja. https://mexico.unir.net/noticias/derecho/derechos-digitales/

ANEXOS

Anexo 1. Matriz completa de las iniciativas de Ley de Ciberseguridad en México.

Iniciativa	Propuesta
Ley de Ciberseguridad para la Ciudad de México Christian Damián Von Roehrich De La Isla (27 de octubre de 2020).	Compuesto por 71 artículos Título 1. Disposiciones Generales Título 2. Obligaciones estructurales en materia de Ciberseguridad Art 8 – 28 Título 3. De las Autoridades Art 29 – 42 · Capítulo I. De la Oficina de Ciberseguridad · Capítulo II. Del Equipo de Inteligencia y Respuesta a Incidentes de Ciberseguridad · Capítulo III. De las Unidades de Ciberseguridad · Capítulo IV. De la Autoridad Investigadora · Capítulo V. De la Fiscalía Especializada en Delincuencia Cibernética Título 4. De las Políticas en materia de Ciberseguridad Art 43 – 44 · Capítulo I De la Política General de Ciberseguridad · Capítulo II De las Políticas Sectoriales de Ciberseguridad

	Título 5. Del Índice, informes y ejercicios, para la mejora continua Art 45-48 · Capítulo I. Del índice · Capítulo II De los informes anuales en materia de Ciberseguridad · Capítulo III De los Ejercicios en materia de Ciberseguridad Título 6. De los Proveedores tecnológicos externos. Art 49-55 Título 7. De la Obligación de cooperación Art 56 Título 8. De la Información en materia de Ciberseguridad Art 57-58 Título 9. De la Asistencia y Cooperación nacional e internacional Art 59-60 Título 10. De Las Responsabilidades En Materia De Ciberseguridad Art 59-60 Responsabilidades (omisión o incumplimiento) Título 11. De Los Delitos En Contra De La Ciberseguridad Con sanción de seis meses a dos años de prisión y de 100 a 500 veces la UMA Delitos dirigidos a las TICS que emplean las Autoridades con la finalidad de afectar el debido ejercicio de la función pública Art. 62. daño al rendimiento y capacidad de las TICS. Art. 63. Interrupción o pérdida de TICS. Art. 64. código malicioso. Art. 65. usurpación de identidad. Art. 66. monitoreo y espionaje. Art. 67. Eliminación y modificación de la Base de datos (ACID). Art. 68. Eliminación y modificación de los controles de seguridad. Art. 69. Filtración y difusión de las Bases de datos. Art. 70. Falsificación de firma digital. Art. 71. Tráfico de información digital.

Ley General de Ciberseguridad Miguel Ángel Mancera Espinosa (1 de septiembre de 2020).	Compuesto por 57 artículos Título 1. Relativo a las Disposiciones Generales, en dicho apartado se encuentra el glosario, así como los diferentes objetos de la ley. Título 2. Concerniente a la Comisión Permanente de Ciberseguridad del Consejo Nacional de Seguridad Pública, en relación con la Ley General del Sistema Nacional de Seguridad Pública (LGSNSP), y quienes podrán participar en ella. Título 3. Contempla el funcionamiento del Centro Nacional de Ciberseguridad sujeto a LGSNSP, en coordinación al Instituto Federal de Telecomunicaciones (IFT), para determinar políticas, lineamientos, mecanismos de evaluación de riesgos y planes de respuestas, que mejoren la gestión de la infraestructura de información crítica Título 4. Nos refiere la seguridad en las operaciones en la red, para ello, el Centro Nacional deberá definir como parte de la Estrategia Nacional de Ciberseguridad un sistema de protección multinivel de ciberseguridad: obligaciones y responsabilidades a los operadores de red para que lleven a cabo actividades comerciales y de servicios; con medidas preventivas y correctivas de seguridad Título 5. Se refiere a las obligaciones del Centro Nacional y operadores de red, y a las responsabilidades de las personas y empresas, en relación a las prevención y erradicación de amenazas cibernéticas y seguridad de la información en la red. Título 6. Se refiere a los proveedores de servicios de ciberseguridad, para tal efecto, el Centro Nacional deberá establecer los requerimientos necesarios para que las empresas proveedoras de ciberseguridad cuenten con los certificados requeridos para la provisión de dichos servicios, de acuerdo con los mejores estándares internacionales en la materia. Título 7. De la Estrategia Nacional de Ciberseguridad que deberá ser desarrollada por el Centro Nacional. Título 8. Lo relativo a los delitos contra la infraestructura informática e Información en sistemas informáticos: · Acceso no autorizado a la información, A cuentas de servicios de Internet, Robo de información y datos personales, Programas malware, troyanos, sniffers, o espías, Acciones ilegales de copia, modificación o uso fraudulento de la información y datos personales, Suplantación de identidad, Gestión de Sitios fraudulentos, Clonación de tarjetas, Contenido digital ilegal, y Alteraciones ilícitas de sistemas de información (infraestructura) y sus respectivas sanciones. · *La multa es por UMA, Se aumenta la pena una tercera parte, sí es una persona servidora pública. Título 9. De la Cooperación Internacional.

Ley General de Ciberseguridad Juanita Guerra Mena (3 de octubre de 2022).	Compuesto por 59 artículos. Título 1. Disposiciones Generales · Capítulo Único Disposiciones Generales Título 2. De Los Ámbitos De Competencia En Ciberseguridad · Capítulo I. Distribución de competencias · Capítulo II. Del Consejo Nacional de Seguridad Pública respecto de la Ciberseguridad · Capítulo III. De la Secretaría de Seguridad y Protección Ciudadana · Sección Primera. De la Dirección General de Investigación Cibernética y Operaciones Tecnológicas · Sección Segunda. De la Policía Cibernética Capítulo IV. De la fiscalía general de Justicia Capítulo V. De los Juzgados Federales Especializados en materia Cibernética Título 3. De la Coordinación De Acciones En Ciberseguridad · Capítulo I De la coordinación entre autoridades competentes en Ciberseguridad · Capítulo II De la coordinación de las autoridades con los sectores de la sociedad · Capítulo III De la coordinación con las Entidades Federativas Título 4. De Las Estrategias Focalizadas De Ciberseguridad · Capítulo I. De las Estrategias · Capítulo II. De los mecanismos de vinculación con autoridades del Sistema Educativo Nacional · Capítulo III. De las políticas públicas, mecanismos y acciones · Capítulo IV. De las garantías de Ciberseguridad a cargo de los proveedores de servicios Título 5. De Las Amenazas, Vulnerabilidades Y Riesgos Por El Uso De Tecnologías De La Información · Capítulo I. Del uso de sistemas informáticos · Capítulo II. De los Perfiles del ciberdelincuente y la ciber víctima Título 6. De La Prevención Y Atención A Los Delitos Cibernéticos · Capítulo Único Del Procedimiento Título 7. De La Promoción Y Formación De Una Cultura De Ciberseguridad · Capítulo I De la participación ciudadana · Capítulo II De la Red de Colaboradores Comunitarios en Ciberseguridad

Ley General de Ciberseguridad Ciudadana Jesús Lucía Trasviña Waldenrath (10 de diciembre de 2024).	Título 8. De Los Convenios Con Entidades Federativas Compuesto por 79 artículos. LIBRO I Título Primero. Disposiciones preliminares Capítulo I Disposiciones Generales Art 1- Art 9 Título Segundo. Política Nacional de Ciberseguridad Capítulo I Principios Rectores Art 10 Capítulo II De la Política Nacional de Ciberseguridad Ciudadana Art 11- Art 13 Capítulo III De la Estrategia Nacional de Ciberseguridad Ciudadana Art 14 – art 15 TÍTULO III. Coordinación y distribución de competencias Capítulo I Distribución de Competencias Art 16 Capítulo II De la Federación Art 17 Capítulo III De la Agencia Nacional de Ciberseguridad Art 18 - art 20 Capítulo IV Del Registro Nacional de Incidentes Cibernéticos Art 21 – art 22 Capítulo V De la Autoridad de Seguridad Ciudadana en Materia Cibernética Art 23 Capítulo VI De las Fiscalías y Procuradurías Art 24 – art 38 capítulo VII De las Autoridades en Seguridad Nacional Art 39- art 41 Capítulo VIII De las Infraestructuras Críticas de Información Art 42 – Art 44 Capítulo IX De los Prestadores de Servicios de Internet y Servicios Web At 45 - Art 47 Capítulo X De la Cibercultura y la Vinculación con Autoridades del Sistema Educativo Nacional Art 48 – Art 49 Capítulo XI De las Entidades Federativas Art 50 Capítulo XII De las Unidades de Policía Cibernética Estatales Art 51 Capítulo XIII facultades y obligaciones de los Municipios Art 52

	Libro Segundo Delitos Cibernéticos Capítulo I De los Delitos contra la Confidencialidad, la Integridad y la Disponibilidad de la Información Art 53 – Art 57 Capítulo II. De los delitos contra el patrimonio Aart 58 Capítulo III. De los delitos contra la libertad de las personas Art 59 – Art 62 Capítulo IV. De los Delitos contra niñas, niños o adolescentes Art 63 – Art 67 Capítulo V. De los delitos contra la violencia de género en el ámbito digital Art 68 – Art 71 Capítulo VI. De los delitos digitales contra la propiedad intelectual Art 72 Capítulo VII. De los delitos contra el Sistema Financiero Art 73- Art 74 Capítulo VIII. Disposiciones comunes a los delitos en materia de las tecnologías de la Información y comunicación, que afectan redes de sistemas informáticos, electrónicos o telemáticos. Art 75 – Art 79
Ley Federal de Ciberseguridad Javier Joaquin López Casarín (20 de marzo de 2024).	Compuesto por 76 artículos Título Primero. Disposiciones Generales Artículo (1-4) Título Segundo. De la Política Nacional de Ciberseguridad Capítulo I. De la Agencia Nacional de Ciberseguridad Artículo (5-10) · Creación de la Agencia Nacional de Ciberseguridad, Dependencia directa del Ejecutivo Federal, Atribuciones Capítulo II. De la Estrategia Nacional de Ciberseguridad Artículo 10 · Diagnóstico nacional, Objetivos estratégicos, Indicadores, Cooperación nacional e internacional, Investigación, formación y desarrollo de industria, Cultura digital Capítulo III. Del Registro Nacional de Incidentes Cibernéticos y Ciberdelitos Artículo (11-13) · Integración del Registro, Administración a cargo de la Agencia, Obligación de reporte Título Tercero. De la Distribución de Competencias Capítulo I. De la Seguridad Nacional Artículo (14-16) · Definición de amenazas a la seguridad nacional en materia cibernética, Obligación de colaboración inmediata, Coordinación entre instancias de seguridad nacional

	Capítulo II. De la Seguridad Pública Artículo (17-22) · Coordinación en el Sistema Nacional de Seguridad Pública, Creación de fiscalía especializada en delitos cibernéticos, Modelo homologado de Policías Cibernéticas estatales, Jueces especializados en cibercrimen Capítulo III. De la Ciberdefensa Artículo (23) · Facultades de la Secretaría de la Defensa Nacional y Secretaría de Marina, Operaciones militares en el ciberespacio · Legítima defensa ante ciber amenazas, Convenios internacionales en materia de ciberdefensa Capítulo IV. De las Infraestructuras Críticas de Información Artículo (24) · Definición de sectores críticos (energía, financiero, salud, transporte, nuclear, etc.), Catálogo Nacional de Infraestructuras Críticas · Obligaciones de responsables: Identificación de activos, Gestión de riesgos, Designación de responsables, Medidas de seguridad, Simulacros y evaluaciones, y Confidencialidad de información Capítulo V. De la Notificación de Incidentes Artículo (33) · Obligación de notificar en máximo 72 horas, Parámetros de impacto (alto, muy alto, crítico), Comunicación al Ministerio Público cuando haya delito Título Cuarto. De la Prestación de Servicios, Uso de Infraestructura Digital y Telecomunicaciones Artículo (37-43) · Obligaciones de Proveedores de servicios de internet, Proveedores de servicios en línea, Servicios bancarios y financieros · Requisitos: Representación legal en México, Plataforma de atención 24/7, Conservación de IP, Suspensión provisional de dominios y Registro ante la Agencia · Registro Nacional de Proveedores de Tecnología para Intervención de Comunicaciones Título Quinto. De la Cultura y Educación Artículo (44-45) Título sexto de las infracciones y sanciones Artículo (46-48) Título séptimo de los delitos cibernéticos Capítulo I. de los Ciberdelitos Sección primera. De los delitos contra la Confidencialidad, Integridad y Disponibilidad de la información Artículo (49-51) Sección segunda. Del ataque a la integridad de un Sistema Informático

	Artículo (52) Sección tercera. A De la interceptación de datos Artículo (53-55) Sección cuarta. De la falsificación informática Artículo (53-56) Sección quinta. Del abuso de dispositivos tecnológicos Artículo (57) Sección sexta. Del fraude por medio informático Artículo (58 - 59) Sección séptima. De los delitos contra la integridad y libertad de las personas Artículo (60-66) Sección octava. De la propiedad intelectual Artículo (67) Sección novena. De los sistemas gubernamentales e infraestructuras críticas de información Artículo (68-73) Capítulo II. De las técnicas especiales de investigación Artículo (74) Capítulo III. Reparación del daño Artículo (75-76)
Ley Federal de Ciberseguridad y Confianza digital Alejandra Lagunes Soto Ruíz (4 de agosto de 2024).	Compuesta por 103 artículos Título Primero. Disposiciones Generales Capítulo Único Artículos (1-5) Título Segundo. Del Sistema Nacional de Ciberseguridad y Confianza Digital Capítulo I. Del Sistema Nacional de Ciberseguridad y Confianza Digital Artículos (6-9) Capítulo II. Del Consejo Nacional de Ciberseguridad Artículos (10-17) Capítulo III. De la Comisión Consultiva de Ciberseguridad Artículos (18-24) Capítulo IV. Del Instituto Nacional de Innovación y Formación en Tecnologías Digitales y Ciberseguridad (INFOTEC) Artículos (25-26) Título Tercero. Estrategia Nacional de Ciberseguridad Capítulo Único Artículos (27-34) Título Cuarto. Marco Regulatorio Capítulo Primero. Sobre el Marco Regulatorio y Competencias

	Artículos (35-45) · Derechos y obligaciones digitales · Marco normativo y Normateca · Protocolos y cumplimiento · Infraestructura crítica y monitoreo · Competencias y estructura institucional Capítulo Segundo. De la Coordinación y Homologación Artículos (46-49) Título Quinto. Combate al Ciberdelito Capítulo Primero. Respeto a los Derechos Humanos en el Ciberespacio Artículos (50-52) · El Consejo establecerá mecanismos de supervisión y control para garantizar el respeto a los derechos humanos en el ciberespacio, en coordinación con autoridades competentes, sociedad civil y actores relevantes, conforme a la legislación nacional y los tratados internacionales suscritos por México. · Se asegurará la prohibición de actividades en el entorno digital que vulneren derechos fundamentales, tales como desinformación dañina, acoso, suplantación de identidad, violaciones a la propiedad intelectual y cualquier forma de violencia o discriminación, sin que las medidas de supervisión limiten derechos humanos. · El Consejo promoverá la educación, concientización y cultura digital basada en el uso responsable y ético de las tecnologías, con apoyo de instituciones académicas y centros de capacitación. Capítulo Segundo. Delimitación de Delitos Artículos (53-56) · Se define el delito cibernético como toda acción u omisión que afecte la confidencialidad, integridad o disponibilidad de datos, sistemas o redes digitales con fines ilícitos o de perjuicio. · Se reconocen diversas conductas típicas en el entorno digital, incluyendo accesos ilícitos, sabotaje, fraude, robo o alteración de información, suplantación de identidad, distribución de malware y explotación de menores, entre otras. · El Consejo analizará y propondrá la actualización de penas y sanciones en el Código Penal Federal, bajo criterios de proporcionalidad. · Se promoverá la cooperación internacional y nacional para la investigación y persecución de delitos cibernéticos. Capítulo Tercero. Figuras Especializadas en Ciberseguridad Artículos (57-60)

	Capítulo Cuarto. Combate al Ciberdelito Artículos (61-64) · El Consejo, en coordinación con la Secretaría de Seguridad y Protección Ciudadana, establecerá y actualizará el Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos, base operativa de la Guardia Cibernética. · El Centro de Respuesta a Incidentes Cibernéticos de la Guardia Nacional fungirá como punto nacional de contacto y apoyo técnico en incidentes que afecten infraestructura crítica. · La Guardia Cibernética operará conforme al Protocolo y a la Estrategia Nacional de Ciberseguridad (Gobierno de México, 2017). · Se establecen líneas de acción en prevención, investigación, persecución, cooperación internacional, desarrollo de capacidades y atención a víctimas. Capítulo Quinto. Registro de Incidentes Cibernéticos Artículos (65-74) · El Consejo regulará y coordinará los Equipos de Respuesta a Incidentes Cibernéticos (CSIRT) para garantizar atención rápida y articulada. · Los CSIRT tendrán funciones de detección, análisis, respuesta, recuperación y asesoría técnica, con colaboración nacional e internacional. · El INFOTEC creará y administrará un Banco de Datos de Incidentes Cibernéticos para análisis estadístico y fortalecimiento de políticas públicas, bajo estrictas medidas de seguridad y confidencialidad. · Se promoverá la adopción de mejores prácticas internacionales, la cooperación internacional y mecanismos de coordinación global. · El reporte de incidentes, sin dolo, no generará responsabilidad por sí mismo.

	Título Sexto. Seguridad Nacional y Protección de Infraestructura Crítica Capítulo Único Artículos (75-84) · Se definen como riesgos e incidentes cibernéticos de seguridad nacional aquellos que comprometan la estabilidad, soberanía o intereses fundamentales del Estado, incluyendo ataques a infraestructura crítica, ciberespionaje, agresiones a instituciones estratégicas y campañas de desestabilización promovidas por actores extranjeros. · Ante estos supuestos, las autoridades del Sistema deberán activar mecanismos de coordinación y respuesta conforme a la legislación aplicable. · La Secretaría de la Defensa Nacional participará en la protección y defensa cibernética cuando exista riesgo a la seguridad nacional, en coordinación con autoridades civiles y bajo protocolos establecidos con el Consejo y el Consejo de Seguridad Nacional. · Se identificará y clasificará la infraestructura crítica del país, estableciendo medidas específicas de protección física y lógica, análisis de riesgos y obligaciones de colaboración por parte de las entidades responsables. · Se crea un registro nacional de incidentes cibernéticos en infraestructuras críticas, con obligación de reporte oportuno y gestión a cargo del Consejo de Seguridad Nacional, bajo estrictos criterios de confidencialidad Título Séptimo. Sobre la Confianza Digital Capítulo Primero. Fomento de la Confianza Digital Artículos (85-91) Capítulo Segundo. Prevención de Campañas de Desinformación Artículo (92) Título Octavo. Uso Ético de Nuevas Tecnologías y Tecnologías Emergentes Capítulo Único Artículos (93-100) Título Noveno. Educación, Capacitación y Cultura Digital Capítulo Único Artículos (101-110)

Anexo 2. Matriz completa de las iniciativas de reforma a la Ley de Seguridad Nacional de México.

Iniciativa	Propuesta
Olga Juliana Elizondo Guerra (7 de abril de 2026).	Artículo 5. Para los efectos de la presente ley, son amenazas a la seguridad nacional: Fracción XIV. Toda acción que tenga como intención, sustraer, dañar, controlar, espiar, inhabilitar o inhibir, el funcionamiento, operaciones, bases de datos, de los sistemas informáticos o redes informáticas de las instituciones del Estado mexicano o de las entidades estratégicas.
María del Rocío Corona Nakamura (3 agosto de 2022).	Artículo 5. Para los efectos de la presente Ley, son amenazas a la Seguridad Nacional: Fracción XIV. Todo acto, conducta, incidente o amenaza ofensiva o maliciosa con la capacidad de provocar un efecto adverso, una falla, un acceso no autorizado, una vulnerabilidad, pérdida, daño o un delito desde el ámbito digital o ciberespacio en contra de las personas, activos, información, infraestructuras de información, tecnologías de operación o instancias e instituciones del Estado Mexicano.
María Eugenia Hernández Pérez (11 de octubre de 2022).	Artículo 5. Para los efectos de la presente Ley, son amenazas a la Seguridad Nacional: Fracción XIV. Actos que tiendan a dañar, interrumpir u obtener acceso no autorizado a la Infraestructura Critica del Estado a través del ciberespacio, con el propósito de interrumpir, deshabilitar, destruir o controlar maliciosamente un entorno o infraestructura de computación, destruir la integridad de los datos o robar la información controlada. Artículo 6. Para los efectos de la presente ley, se entiende por: Fracción VII. Ciberespacio: Dominio global dentro del entorno de la información que consiste en una red interdependiente de infraestructuras de TI, incluyendo Internet, redes de telecomunicaciones, sistemas informáticos y procesadores embebidos y controladores. Artículo 13. El Consejo de Seguridad Nacional es una instancia deliberativa cuya finalidad es establecer y articular la política en la materia. Por tanto, conocerá los asuntos siguientes: Fracción IX. Los procesos de clasificación, desclasificación y resguardo de información en materia de seguridad nacional.

Cora Cecilia-Pinedo Alonso (7 de diciembre de 2022).	Artículo 5. Para los efectos de la presente Ley, son amenazas a la Seguridad Nacional: Fracción XIV. Actos tendentes a destruir, inhabilitar u obstaculizar, las medidas de Ciberseguridad, que protegen la información y datos personales en posesión de instituciones públicas y privadas, los sistemas informáticos que garantizan la prestación de servicios de instituciones públicas y privadas. Articulo 6.- Para los efectos de la presente Ley, se entiende por: Fracción VIII. Ciberseguridad: Conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger al gobierno, a la sociedad y seguridad nacional en el ciber entorno.
Miguel Ángel Mancera Espinosa (1 de septiembre de 2020).	Artículo 5. Para los efectos de la presente Ley, son amenazas a la Seguridad Nacional: Fracción XIV. Actos tendentes a amenazar, afectar, inhabilitar o destruir la infraestructura activa o pasiva de telecomunicaciones que sean indispensable para la provisión de bienes o servicios públicos o para el adecuado funcionamiento de las instituciones del Estado.

Anexo 3. La organización y su contexto

Indicaciones:

- La evaluación del nivel de madurez se obtiene mediante el promedio de los subcomponentes que integran cada componente.
- Escala de madurez: 1 = Inexistente; 2 = Básico; 3 = Medible; 4 = Optimizado.
- Tipos de hallazgo: C = Conformidad; CC = Conformidad Condicionada; NC = No Conformidad.

REPORTE INTEGRAL EN CUMPLIMIENTO CON LA NORMA ISO27001. Cláusula 4. La organización y su contexto		
Institución / organización:		Folio: 1/N
Área o Proceso Auditado:		Fecha: / /25
Responsable del Área:		Auditoria: Externa
Asesor Auditor:		
4.1	Comprender la organización y su contexto	Nivel de Madurez: 2
A	¿Cómo podrían verse afectadas la confidencialidad, la integridad y la disponibilidad de la información?	
La implementación inadecuada o la ausencia de controles de acceso robustos, como contraseñas débiles, falta de autenticación multifactor o permisos excesivos a usuarios, podría comprometer la confidencialidad al permitir que personas no autorizadas accedan a información sensible. Adicionalmente, la falta de mecanismos de control de versiones del sistema y auditoría podría afectar la integridad, dificultando la detección y corrección de modificaciones no autorizadas a los datos. Finalmente, la ausencia de planes de contingencia y recuperación ante desastres, como copias de seguridad regulares y sitios de respaldo, podría impactar la disponibilidad de la información en caso de fallos del sistema, ataques o eventos inesperados		

No.	Hallazgo	Tipo	Evidencia	Recomendaciones	Riesgo	Nivel
1	Es inadecuado el protocolo de actuación para el desecho de los recursos tecnológicos en específico, discos duros interno, externos, de respaldo, memorias extraíbles, cuentas de usuarios.	OM	Los recursos tecnológicos son formateados y posteriormente desechados en el sistema de recolección municipal de basura	Destrucción física de los dispositivos de almacenamiento, procesamiento y cuentas de usuarios, antes de desechar el recurso, alternativas: imantación, trituración y soluciones químicas	La información puede recuperar con formato de bajo nivel, exponiendo la confidencialidad de los datos	2
B	¿Cuál es el valor agregado de los activos de información para la Organización?					
El valor agregado de los activos de información se manifiesta en la reducción cuantificable del riesgo, a mediante planes de continuidad y recuperación robusta, la reducción del número de incidentes mediante sistemas de detección y prevención de intrusiones, gestión de vulnerabilidades y concienciación del personal, y la mejora en la eficiencia de los procesos de negocio (gracias a la disponibilidad e integridad de los datos críticos, respaldada por controles de acceso granular que limitan el acceso a la información a los usuarios y procesos autorizados. y la auditoría de los accesos y modificaciones a datos críticos con una trazabilidad que permite identificar y corregir cualquier anomalía					
No.	**Hallazgo**	**Tipo**	**Evidencia**	**Recomendaciones**	**Riesgo**	**Nivel**
1	Existe un plan de administración de riesgo	C	El plan de riesgo considera las áreas de tecnologías, recursos e infraestructura	Actualizar y difundir	Un plan no actualizado no contempla nuevas amenazas y los costos de impacto	3
2	No existen un control de trazabilidad en las operaciones	NC	Las operaciones se realizan sin el registro de los usuarios, día, hora, y los datos que se actualizan	Implementar una bitácora que lleve el registro de todas las operaciones que se realizan	Cualquier persona puede ingresar sin dejar un rastro de las operaciones que realiza y esto puede detonar en actividades ilícitas	1
C	¿Qué impacto tendría una divulgación involuntaria? ¿Qué supondría un evento o incidente?					

Una divulgación involuntaria expondría datos sensibles (personales, financieros, propiedad intelectual) a entidades no autorizadas, desencadenando fugas masivas, suplantación de identidad y pérdidas económicas por fraude o sanciones regulatorias (GDPR, HIPAA). Esto exige controles de acceso robustos (RBAC, ABAC), cifrado fuerte en reposo y tránsito (AES-256, TLS 1.3), y soluciones de Prevención de Pérdida de Datos (DLP). Un evento de intrusión detectada por un Sistema de Detección y Prevención de Intrusiones (IDS/IPS) señala una brecha en las defensas perimetrales, requiriendo la respuesta inmediata de un plan de respuesta a incidentes (IRP). Si este evento escala a incidente confirmado (exfiltración de datos, denegación de servicio sostenida), supondría la materialización de riesgos, demandando la activación inmediata del IRP, la ejecución de análisis forense digital para determinar la causa raíz y alcance, y la implementación de medidas correctivas robustas, incluyendo el endurecimiento de sistemas, la aplicación de parches de seguridad oportunos y la revisión exhaustiva de la arquitectura de seguridad

No.	Hallazgo	Tipo	Evidencia	Recomendaciones	Riesgo	Nivel
1	Sin hallazgo	C	Documentado, actualizado, revisión continua; no obstante	Continuar con el mismo proceso	No aplica	4

D	¿Cuál sería el impacto de la pérdida de confianza en la integridad de su información? Por ejemplo, la integridad del registro del cliente.

La pérdida de integridad en datos críticos (ej., registro de clientes) se origina técnicamente por fallas en DBMS, accesos indebidos, validación débil o falta de auditoría. Las buenas prácticas exigen DBMS seguros y parcheados, RBAC y el principio de mínimo privilegio, la adopción de mecanismos de validación de datos en la entrada y durante el procesamiento, la implementación de auditorías exhaustivas de las modificaciones a los datos, la realización de copias de seguridad periódicas y la implementación de mecanismos de detección como checksums, y firmas digitales para asegurar la confiabilidad y la validez de la información crítica

No.	Hallazgo	Tipo	Evidencia	Recomendaciones	Riesgo	Nivel
1						

E	¿Qué consecuencias tendría una divulgación involuntaria de información en un acuerdo de subcontratación o en el extranjero? ¿Cuáles son las fuentes de riesgo? ¿Qué amenazas hay?

Divulgar información en subcontratación o en el extranjero tendría consecuencias técnicas, legales y reputacionales significativas, la información sensible (datos personales, propiedad intelectual, secretos comerciales) quedaría expuesta a sistemas y redes fuera del control directo de la organización, aumentando la dificultad para rastrear y contener, por vulnerabilidades de terceros, configuraciones inseguras en sus sistemas o transferencias sin cifrado. El riesgo surge de la seguridad potencialmente menor del subcontratista, políticas desalineadas, accesos inadecuados, empleados con acceso indebido y la jurisdicción extranjera. Las amenazas incluyen ataques a la cadena de suministro, ingeniería social a empleados del subcontratista, espionaje facilitado por la ubicación y negligencia o incidentes en su sistema

No.	Hallazgo	Tipo	Evidencia objetiva	Recomendaciones	Riesgo	Nivel
1						
4.2	Comprender las necesidades y expectativas de las partes interesadas				Nivel de Madurez: 2	
A	¿Cómo podrían verse afectados los socios, clientes, proveedores y empleados por la falta de controles de seguridad de la información o actividades de continuidad de negocios?					

Una brecha, ante la ausencia de cifrado robusto en reposo y tránsito (AES-256, TLS 1.3), controles de acceso basados en roles (RBAC) y autenticación multifactor (MFA), expondría datos sensibles de clientes (personales, financieros), derivando en pérdidas económicas y robo de identidad.

Para socios y proveedores, la falta de acuerdos de confidencialidad (NDA) y canales de comunicación seguros (VPN) comprometería su información compartida.

La ausencia de planes de recuperación ante desastres (DRP) con sitios alternos y copias de seguridad periódicas y verificadas interrumpiría la cadena de suministro de proveedores y la operatividad interna, afectando a los empleados por la inactividad y la exposición de sus datos personales ante la falta de DLP y políticas de borrado seguro.

No.	Hallazgo	Tipo	Evidencia	Recomendaciones	Riesgo	Nivel
1						
B	¿Cómo podrían verse afectada la seguridad de la información o continuidad del negocio sí fueran los socios, clientes, proveedores y empleados los responsables de las malas prácticas?					

Si los empleados ignoran las políticas de seguridad, hicieran clic en enlaces maliciosos o no protegieran sus dispositivos personales, serían la causa directa de infecciones de malware y fugas de datos. Si los socios y proveedores, por negligencia en la implementación de protocolos de comunicación seguros o en la protección de las API de integración, fueran la causa de exposición de información compartida o la interrupción de servicios críticos. Si los clientes, mediante prácticas de autenticación débiles o el compromiso de sus cuentas, permitieran accesos no autorizados a la plataforma o datos de otros clientes. Y si ninguno de los stakeholders tomará medidas básicas de respaldo de la información o no siguiera los planes de continuidad definidos (si existieran), la suspensión de actividades esenciales tras un incidente (fallo de sistema, ataque) sería una consecuencia directa de su inacción o incumplimiento.

No.	Hallazgo	Tipo	Evidencia	Recomendaciones	Riesgo	Nivel
1						
C	¿Considera que los procesos actuales cumplen con las leyes y regulaciones emitidas por agencias gubernamentales y entidades reguladoras en materia de protección de datos personales y seguridad de la información?					

Se identificaron incumplimientos en las normativas de protección de datos personales y seguridad de la información. Aunque los procesos incluyen lineamientos básicos, la organización carece de un aviso de privacidad integral y simplificado, como lo exige la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPSO). Esto impide informar adecuadamente a los titulares sobre el uso, tratamiento y finalidades de sus datos personales. Además, la organización no ha incorporado mecanismos de seguridad esenciales, como el cifrado robusto (AES-256) y el control de acceso basado en roles (RBAC), requeridos por la norma ISO/IEC 27001 y alineados con las disposiciones de la LGPDPSO en su artículo 28, que obliga a implementar medidas técnicas, administrativas y físicas para proteger los datos personales contra daño, pérdi-da, alteración y acceso no autorizado.

También, la falta de mecanismos para garantizar el ejercicio de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), la ausencia de auditorías regulares y la falta de registros sobre el consentimiento explícito para el tratamiento de datos colocan a la organización en una situación de riesgo frente a sanciones regulatorias. Esto inclu-ye impactos reputacionales significativos, así como la pérdida de confianza de clientes, socios y proveedores.

No.	Hallazgo	Tipo	Evidencia	Recomendaciones	Riesgo	Nivel
1						
4.3.	Determinación del Alcance del Sistema de Gestión de Seguridad de la Información SGSI					
A	¿Qué productos y servicios en su organización estarán cubiertos por el SGSI?					

El alcance del SGSI se define considerando productos y servicios que almacenan, procesan o transmiten información crítica o sensible. Se incluyen plataformas de almacenamiento y bases de datos, servicios de autenticación (Active Directory, LDAP, MFA, IAM), infraestructura de red (firewalls, IDS/IPS, switches, routers), aplicaciones web y móviles (con controles de SDLC seguro y pruebas de seguridad), servicios de correo electrónico (con cifrado S/MIME o PGP, políticas DLP), procesos de gestión de incidentes (con roles definidos y herramientas de seguimiento), y actividades de continuidad de negocio (planes DRP, sitios alternos, pruebas de failover/failback). Estos elementos definen los límites operativos y tecnológicos del SGSI conforme a su impacto sobre los activos de información.

No.	Hallazgo	Tipo	Evidencia	Recomendaciones	Riesgo	Nivel
1						
B	¿Si las actividades realizadas por la organización requieren de interfaces o dependencias externas o de actividades realizados por terceros? ¿Deberían ser considerados dentro del alcance del SGSI					

Las interfaces externas, como ISP, proveedores cloud y socios estratégicos, introducen riesgos técnicos por vulnerabilidades en sus sistemas, prácticas de seguridad inadecuadas, transferencias de datos sin cifrado y cumplimiento normativo disparejo.

Para gestionarlos, el SGSI debe incorporar evaluaciones de terceros (Due Diligence), cláusulas contractuales de seguridad, cifrado fuerte en tránsito y reposo, controles de acceso, auditorías periódicas y planes de contingencia coordinados. Estas medidas permiten extender el perímetro de seguridad y reducir la exposición a amenazas externas.

No.	Hallazgo	Tipo	Evidencia	Recomendaciones	Riesgo	Nivel
1						
C	¿Cómo identifica y justifica que un producto o servicio es crítico para su organización, considerando sus características principales como negocio, ubicaciones, activos, tecnologías, y si requiere que proveedores externos cumplan con el SGSI?					
La supervisión del SGSI presenta debilidades debido a la falta de herramientas técnicas clave. No se implementaron soluciones SIEM para monitoreo en tiempo real, ni controles DLP para prevenir fuga de información. Tampoco existen dashboards integrados con KPI de riesgos o cumplimiento normativo, ni auditorías internas formales bajo ISO/IEC 27001. Adicionalmente, no se realizan validaciones técnicas como pruebas de penetración o simulacros de respuesta a incidentes, lo cual limita la capacidad de detección de fallas y evaluación de resiliencia ante amenazas emergentes. Esta carencia afecta la eficacia y mejora continua del SGSI.						
No.	**Hallazgo**	**Tipo**	**Evidencia**	**Recomendaciones**	**Riesgo**	**Nivel**
1						
Auditor						
Nombre de identificación						

Identificar el tipo de hallazgo:

(NC) No Conformidad: Incumplimiento total o parcial de un requisito establecido en la norma ISO/IEC 27001, en la normativa aplicable o en las políticas, procedimientos y controles internos de la organización. Requiere la implementación de acciones correctivas.

(CC) Conformidad Condicionada: El requisito evaluado se cumple; sin embargo, presenta oportunidades de mejora que fortalecen su eficacia, documentación, implementación o seguimiento, sin constituir un incumplimiento de la norma

(C) Conformidad: El requisito se cumple plenamente y existe evidencia objetiva suficiente de su implementación y eficacia

Anexo 4. Manual de Políticas de Seguridad Informática

Versión: 1.0 Fecha de emisión: 5/mayo/2025
Coordinación: Dirección de Seguridad de la Información

Introducción

Este manual establece las políticas, especificaciones y lineamientos necesarios para garantizar la seguridad y la protección de la información, los activos digitales y los sistemas tecnológicos de la institución. Su elaboración se basa en las normas internacionales ISO/IEC 27001 y 27002, integrando buenas prácticas de las normas ISO 14001 (gestión ambiental) e ISO 50001 (gestión de la energía).

.

SECCIÓN I: Marco General

1. Fundamento y Establecimiento de Políticas

La seguridad informática es un componente esencial para la protección de los activos de información de la organización. Las políticas de seguridad deben ser establecidas por la Alta Dirección, con base en los siguientes lineamientos:

- Estar alineadas con la visión global del negocio y los objetivos estratégicos institucionales.
- Corroborar su cumplimiento mediante auditorías internas, métricas e indicadores de control.
- Asegurar que reflejen el alcance y misión del área de informática dentro de la organización.
- Integrar controles en todas las áreas de negocio, permitiendo un enfoque transversal y coordinado.
- Permitir que los distintos departamentos generen políticas internas complementarias, siempre que estén alineadas con las políticas organizacionales y validadas por la Dirección correspondiente.

2. Importancia de una Política de Seguridad Informática

Las políticas de seguridad informática son instrumentos normativos que permiten a la organización:

- Comunicarse de manera efectiva con los usuarios, estableciendo claramente las normas de actuación respecto al uso de los recursos tecnológicos.
- Prevenir incidentes relacionados con accesos no autorizados, uso indebido de información o afectación de la infraestructura digital.
- Establecer de forma explícita las responsabilidades, especificaciones y excepciones, junto con las sanciones aplicables en caso de incumplimiento.
- Fomentar una cultura organizacional basada en la protección de los sistemas de información.
- Deben redactarse en un lenguaje claro y directo, evitando tecnicismos o términos ambiguos que puedan prestarse a interpretaciones subjetivas o parciales.
- Las excepciones, deben ser aprobadas por el responsable de seguridad de la información, de forma escrita con tiempo determinado y en atención a una justificación técnica o funcional válida.

3. Distribución, Publicación, Aplicación y Actualización

- Todas las políticas deben ser distribuidas oficialmente a través de los canales institucionales.
- Su versión vigente debe permanecer publicada en un repositorio digital accesible para todos los colaboradores.
- La aplicación es obligatoria desde la fecha indicada y su desconocimiento no exime de responsabilidad.

- Se deben revisar anualmente o cuando ocurra una modificación sustancial en el entorno legal, técnico o organizacional.
- Cada política incluirá una tabla de control de cambios y la designación del responsable de su mantenimiento.

4. Base Normativa

En el control de cambios del 2026, Anexar otras normas y leyes, en atención a las nuevas políticas.

- ISO/IEC 27001:2022 – Sistema de Gestión de Seguridad de la Información.
- ISO/IEC 27002:2022 – Controles de Seguridad de la Información.
- Legislación nacional en materia de protección de datos y delitos informáticos.
- Reglamento Interno de Trabajo.
- Manual de Normas y Procedimientos de Tecnología.
- Definiciones Clave
- Recurso tecnológico: Cualquier activo informático bajo control de la organización: hardware, software, redes, sistemas, servicios digitales o información almacenada.
- Especificación: Lista autorizada o criterio técnico formalmente definido por el área de TI.
- Excepción: Situación puntual que no aplica la norma general, debidamente autorizada por el área correspondiente.
- Evento de seguridad: Toda anomalía detectada en el comportamiento de los sistemas que pueda representar una amenaza a la confidencialidad, integridad o disponibilidad de la información.
- Activo informático: Todo recurso físico o digital con valor para la institución.

SECCIÓN II: Resumen Operativo y Técnico de Políticas de Seguridad Informática

A continuación, se presentan los resúmenes operativos y técnicos correspondientes a políticas de seguridad de la información. Cada uno cumple una función introductoria que orienta sobre el propósito funcional de la política, su relevancia en los procesos institucionales y el impacto técnico que conlleva su correcta aplicación. Estos deben entenderse como puntos de partida para el desarrollo detallado de cada política, tomando como guía los lineamientos establecidos en el presente manual.

21. Uso Responsable de los Recursos Tecnológicos

- Resumen operativo: Establece las reglas para el uso adecuado, seguro y exclusivamente institucional de los recursos tecnológicos, promoviendo su utilización responsable por parte del personal autorizado para proteger la información, garantizar la continuidad de las operaciones y prevenir usos indebidos.
- Resumen técnico: Define controles administrativos, técnicos y organizacionales para el uso de equipos, redes, sistemas, aplicaciones y servicios digitales, conforme a los principios de uso aceptable establecidos en ISO/IEC 27001 e ISO/IEC 27002 (controles relativos al uso de activos, comportamiento seguro del usuario y protección de la información), fortaleciendo la disponibilidad, integridad y confidencialidad de los activos tecnológicos mediante mecanismos de supervisión, monitoreo y cumplimiento normativo.

2.2 Acceso a Sistemas Institucionales

- Resumen operativo: Regula el ingreso autorizado a plataformas digitales mediante cuentas institucionales y obliga al cierre de sesión tras su uso.
- Resumen técnico: Implementa controles de identi-dad, autenticación segura y privilegios mínimos (ISO/ IEC 27001 A.9.1), con auditoría de accesos y revocación automatizada.

2.3 Acceso Físico a Instalaciones Tecnológicas

- Resumen operativo: Controla la entrada a laboratorios, centros de datos, oficinas de TI y espacios restringidos.
- Resumen técnico: Aplica medidas como credenciales físicas, cerraduras electrónicas, bitácoras de acceso y videovigilancia conforme ISO/IEC 27002 A.11.1.

2.4 Manejo de Información y Datos Personales

- Resumen operativo: Asegura que toda información sensible o personal sea tratada con confidencialidad y legalidad.
- Resumen técnico: Cumple con la Ley Federal de Protección de Datos (México), RGPD y las cláusulas 8.2 y 18.1 de ISO/IEC 27001.

2.5. Inicio y Cierre de Sesión

- Resumen operativo: Obliga a cerrar sesión en sistemas al finalizar el uso, evitando accesos indebidos en terminales compartidas.
- Resumen técnico: Permite trazabilidad completa mediante logs. Las sesiones inactivas deben cerrarse automáticamente (ISO/IEC 27002 A.9.4.2).

2.6 Instalación de Software

- Resumen operativo: Solo se permite software autorizado; se documentan excepciones con justificación técnica.
- Resumen técnico: Se exige control de licencias, validación de proveedores y registro de instalación. Aplica ISO/IEC 27002 A.12.5.

2.7 Uso de Internet Institucional

- Resumen operativo: Delimita qué tipo de contenido está permitido y regula el uso recreativo o personal de la red.
- Resumen técnico: Se establece filtrado de contenido, control de tráfico y monitoreo con respaldo legal (ISO/IEC 27002 A.13.1.1).

2.8 Uso de Plataformas de Inteligencia Artificial

- Resumen operativo: Autoriza su uso con fines educativos o institucionales, bajo supervisión y respeto a privacidad.
- Resumen técnico: Se aplican criterios éticos, revisión de fuentes y prohibición de uso no controlado, conforme a recomendaciones de UNESCO e ISO/IEC 23894 (ética en IA).

2.9 Correo Electrónico Institucional

- Resumen operativo: Prohíbe el uso personal intensivo, spam, o compartir credenciales del correo institucional.
- Resumen técnico: Se monitorean mensajes salientes, se filtran adjuntos y se previene phishing mediante DMARC, SPF y DKIM. Aplica ISO/IEC 27002 A.13.2.3.

2.10 Dispositivos de Almacenamiento Externo

- Resumen operativo: Toda memoria USB o disco externo debe escanearse con antivirus y preferentemente cifrarse.
- Resumen técnico: Se regula el uso con protocolos de control de dispositivos (DLP), cifrado AES y políticas de prevención de pérdida (ISO/IEC 27002 A.8.3.3).

2.11 Registro, Monitoreo y Auditoría de Actividades

- Resumen operativo: Toda actividad digital en sistemas institucionales puede ser registrada bajo principios de legalidad y proporcionalidad.
- Resumen técnico: Logs, alertas y reportes de auditoría se conservan por 12 meses. Se sigue ISO/IEC 27001 A.12.4 y NIST SP 800-92.

2.12 Resguardo y Respaldo de Información

- Resumen operativo: Todo sistema debe respaldarse semanalmente y los respaldos deben almacenarse de forma segura.

- Resumen técnico: Se aplican mecanismos de backup incremental, pruebas de restauración y almacenamiento cifrado (ISO/IEC 27001 A.12.3).

2.13 Actualización y Parches de Seguridad

- Resumen operativo: Todo software debe actualizarse mensualmente; se priorizan vulnerabilidades críticas.
- Resumen técnico: Aplicación de parches mediante MDM o WSUS, con documentación del ciclo de revisión. ISO/IEC 27002 A.12.6.1.

2.14 Eliminación y Destrucción de Información

- Resumen operativo: La baja de equipos o discos debe incluir borrado seguro o destrucción física del medio.
- Resumen técnico: Se utilizan técnicas como DoD 5220.22-M, desmagnetización o destrucción mecánica (ISO/IEC 27040).

2.15 Gestión de Residuos Tecnológicos

- Resumen operativo: Se deben clasificar, documen-tar y entregar a recicladores certificados los residuos electrónicos.
- Resumen técnico: Aplica la ISO 14001 y la Ley General para la Prevención y Gestión Integral de Residuos (México) para evitar impactos ambientales y filtraciones de datos.

2.16 Gestión Energética de los Recursos TI

- Resumen operativo: Se fomenta el uso eficiente de energía: apagado programado, reducción de consumo, migración a equipos eficientes.
- Resumen técnico: Implementación de ISO 50001 en centros de datos, oficinas y servidores. Uso de medidores inteligentes y prácticas de eficiencia energética.

2.17 Derechos y Responsabilidades Digitales del Personal Técnico

- Resumen operativo: Define qué pueden y no pueden hacer los administradores con acceso privilegiado.
- Resumen técnico: Obliga a documentar acciones, respetar la privacidad, usar cuentas diferenciadas y generar trazabilidad (ISO/IEC 27001 A.9.2 y RGPD).

2.18 Prevención de Violencia Digital en Entornos Institucionales

- Resumen operativo: Prohíbe ciberacoso, suplantación de identidad y uso hostil de plataformas institucionales.
- Resumen técnico: Basado en la Ley Olimpia (México), ISO/IEC 27002 cláusula 7.2.2, y principios de dignidad digital. Se promueve canal de denuncias y monitoreo activo.

2.19 Cultura Digital y Ciberresiliencia del Usuario

- Resumen operativo: Promueve capacitación continua, simulacros, y formación en buenas prácticas digitales.
- Resumen técnico: Aplica ISO/IEC 27001 A.7.2.2, ISO/IEC 27031 (ciberresiliencia) y 27002. Incluye planes de concientización y respuestas ante incidentes

SECCIÓN III: Políticas de Seguridad Informática

Las políticas de seguridad informática son lineamientos institucionales que regulan el uso, protección y gestión de los recursos tecnológicos de la organización. Su objetivo es minimizar riesgos, proteger la información y garantizar la continuidad operativa, definiendo con precisión las responsabilidades, especificaciones y excepciones, para construir no solo sistemas seguros, sino una cultura digital resiliente, ética y consciente.

31. Uso Responsable de los Recursos Tecnológicos

Versión: 1.2 Fecha de entrada en vigor: 5/mayo/2025

Revisión prevista: 5/mayo/2026

A. Objetivo

Establecer los lineamientos específicos para el uso adecuado de los recursos tecnológicos institucionales, con el fin de garantizar la seguridad de la información, la continuidad operativa y el cumplimiento de las funciones laborales en el marco de la normativa vigente.

B. Alcance

Aplica a todo el personal interno o externo que, bajo cualquier relación laboral o contractual, tenga acceso a equipos, plataformas, redes o servicios informáticos de la organización, en modalidad presencial o remota.

C. Responsabilidad

El personal debe utilizar los recursos tecnológicos institucionales exclusivamente para el cumplimiento de sus funciones laborales, conforme a los objetivos operativos de su unidad.

D. Especificación

- El uso de hardware, software, red y servicios digita-les debe limitarse a tareas descritas en el Manual de Funciones de cada unidad.
- Está prohibido utilizar dispositivos institucionales para actividades personales, comerciales, políticas, religiosas o ajenas a la organización.
- Solo podrán utilizarse plataformas, servicios de mensajería y aplicaciones previamente autorizadas por el área de Tecnología.
- Las conexiones remotas deberán realizarse en el horario laboral oficial y mediante los mecanismos aprobados de acceso seguro.
- Cualquier configuración, instalación o modificación de equipos o sistemas requiere autorización expresa del área de Tecnología.

E. Excepción

- Se permite el uso del equipo institucional con fines personales únicamente durante tiempos de receso (pausas laborales), limitado a navegación web no riesgosa, sin instalación de programas ni transferencia de archivos personales. – con observación en el tráfico de datos-
- El uso de software o herramientas no institucionales será autorizado temporalmente solo si:
- a) están directamente vinculadas con procesos de capacitación, evaluación o mantenimiento.
- b) existe una justificación técnica o funcional documentada, y c) cuentan con aprobación escrita del área de Tecnología y de Seguridad de la Información.
- Toda excepción tendrá una vigencia máxima de 30 días calendario, con opción de renovación mediante nueva solicitud formal justificada.

F. Sanciones

Nivel	Infracción	Sanción Aplicable	Procedimiento Disciplinario
Leve	Uso personal injustificado durante horas laborales	Amonestación por escrito	Registro en expediente; aviso formal a Recursos Humanos
Media	Uso de software no autorizado sin aprobación	Suspensión temporal de acceso hasta por 5 días hábiles	Informe técnico a Seguridad de la Información; audiencia breve con supervisor inmediato
Grave	Instalación de programas maliciosos o filtración de información institucional	Terminación del contrato, denuncia legal y bloqueo de acceso	Investigación formal por el Comité de Ética o Jurídico; reporte a Dirección General y RH

Control de Cambios

Versión: 1.0

Fecha: 5 de mayo de 2025

Ciberseguridad y Gobernanza en la Era Digital

se terminó de editar en septiembre de 2026,
en Tuxtla Gutiérrez, Chiapas.