Los estándares internacionales y el fortalecimiento de la ciberseguridad en la industria

GPQI
Dialogues for Innovation and Trade

Publicado por
Deutsche Gesellschaft für
Internationale Zusammenarbeit (GIZ) GmbH

Oficinas registradas
Bonn y Eschborn, Alemania.

Global Project Quality Infrastructure
Agustín González de Cossío No. 821
Col. del Valle Centro, 03100
Ciudad de México, México

Diseño
Pamela Parra
Pam Parra Graphic Design, CDMX, México

Créditos fotográficos
Título: Freepik

Por encargo de
Ministerio Federal de Economía y Protección del Clima (BMWK) de Alemania
Berlín, Alemania, 2023
Ciudad de México, México, 2023

Texto
Proyecto Global Infraestructura de la Calidad (Global Project Quality Infrastructure, GPQI)

El Ministerio Federal de Economía y Protección del Clima (BMWK) de Alemania comisionó a la Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH para la implementación del Proyecto Global Infraestructura de la Calidad (Global Project Quality Infrastructure, GPQI).

Implemented by

Con el apoyo de

- Asociación de Internet MX
- Asociación Mexicana de la Industria de Tecnologías de Información (AMITI)
- Asociación de Normalización y Certificación (ANCE)
- Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI)
- Centro de Investigaciones sobre América del Norte
- Deutsche Kommission Elektrotechnik (DKE)
- Instituto Federal de Telecomunicaciones (IFT)
- Normalización y Certificación NYCE, SC
- SAP
- Secretaría de Economía
- Secretaría de Infraestructura, Comunicaciones y Transportes (SICT)
- Secretaría de Seguridad y Protección Ciudadana (SSPC)
- Siemens
- TMI Abogados
- TÜV Rheinland

Sobre esta publicación

Esta publicación se desarrolló en el marco del Diálogo Mexicano–Alemán en Infraestructura de la Calidad, establecido entre el Ministerio Federal de Economía y Protección del Clima de Alemania (BMWK) y la Secretaría de Economía de México. Este diálogo bilateral es una plataforma que reúne a representantes de ministerios relevantes, instituciones de infraestructura de la calidad, empresas, así como asociaciones y cámaras industriales de ambos países para abordar temas de cooperación de interés mutuo en materia de infraestructura de la calidad.

En el marco del Proyecto Global Infraestructura de la Calidad (GPQI, por sus siglas en inglés), el BMWK participa en diálogos político-técnicos con importantes socios comerciales de todo el mundo. Este proyecto se lleva a cabo con el apoyo de la Cooperación Técnica Alemana (GIZ) y en colaboración con Brasil, China, India, Indonesia y México.

Esta publicación es el resultado de un trabajo en conjunto desde 2021 entre actores del grupo bilateral de expertos dentro de la línea de proyecto "Ciberseguridad en el contexto de la digitalización y la Industria 4.0", acordada en el plan de trabajo conjunto del Diálogo Mexicano–Alemán en Infraestructura de la Calidad. Esta línea de proyecto tiene como objetivo reforzar la aplicación de estándares armonizados internacionalmente en el ámbito de la ciberseguridad y la seguridad de la información con la finalidad de garantizar cadenas globales de valor que sean seguras y resilientes.

Este segundo volumen presenta un mapeo de los estándares internacionales más importantes, de manera que pueda ser una guía para las empresas sobre estas herramientas para la gestión de la ciberseguridad y sus beneficios. Dicha serie se integra por las siguientes publicaciones: (1) La importancia de la ciberseguridad en la transformación digital de las empresas; (2) Los estándares internacionales y el fortalecimiento de la ciberseguridad en la industria; (3) Recomendaciones a las autoridades regulatorias: Fortaleciendo el uso de estándares internacionales de ciberseguridad en el sector privado mexicano; y (4) Guía de implementación de medidas de Ciberseguridad para empresas.

Contenido

1. Introducción

// En una economía cada vez más interconectada y digitalizada, la ciberseguridad se ha convertido en una prioridad fundamental para empresas de todos los sectores y tamaños. Debido a la creciente sofisticación de las amenazas cibernéticas y la constante evolución del panorama de seguridad, el contar con un enfoque sólido y estructurado es esencial para proteger los activos digitales y garantizar la confidencialidad, integridad y disponibilidad de la información.

En este contexto, los estándares internacionales de ciberseguridad desempeñan un papel crucial al ser los que proporcionan las pautas, buenas prácticas y marcos de referencia para que las organizaciones puedan diseñar, desarrollar, implementar y mantener estrategias efectivas de protección cibernética. Además, ofrecen una estructura coherente y reconocida a nivel global, permitiendo a las empresas adaptarse a las amenazas cambiantes y cumplir con las regulaciones aplicables.

Este documento tiene como objetivo explorar los principales estándares internacionales de ciberseguridad que han sido ampliamente adoptados por organizaciones y empresas en todo el mundo. En él se examinan las características distintivas que definen a los múltiples estándares en materia de ciberseguridad y seguridad de la información. De igual forma, es un complemento a la "Guía de implementación de medidas de ciberseguridad para empresas", publicada en el marco de esta misma serie de documentos, donde se explican a detalle temas como gestión de riesgos, concientización sobre la ciberseguridad y capacitación del personal dentro de las empresas, diferentes tipos de controles y herramientas de protección, consideraciones específicas para la ciberseguridad en aplicaciones en la nube y redes industriales, así como los pasos a seguir para lograr una gestión eficaz de incidentes.

© Diloka107/Freepik

El presente documento busca complementar dicha Guía a través del mapeo y la descripción de los estándares internacionales que son considerados más importantes, para así ayudar a fortalecer los procesos de gestión de ciberseguridad de las organizaciones. Asimismo, pretende brindar una orientación a las Pequeñas y Medianas Empresas (PyMEs) en la implementación de dichos estándares y, con ello, contribuir a generar un ecosistema empresarial e industrial más seguro y resiliente.

A partir de una introducción a los estándares internacionales, su aplicación y sus beneficios, se presentan aquellos que son más destacados en materia de ciberseguridad según su función, empezando por los que contienen definiciones relevantes, para continuar con los estándares de gestión de riesgos, de técnicas de control e implementación generales y aplicadas a tecnologías específicas como la nube y las redes industriales, y cerrar con aquellos que definen los lineamientos para la gestión de incidentes.

Adicionalmente, en los anexos se encuentran una serie de insumos complementarios como es un listado de las regulaciones más importantes en materia de ciberseguridad en México (Anexo 1, "Marco legal: leyes en México relacionadas a la ciberseguridad"), seguido por el listado completo de los estándares internacionales presentados

en el texto y organizados por temáticas (Anexo 2, "Estándares internacionales de ciberseguridad"). En el Anexo 3 ("Estándares de ciberseguridad para sectores y actividades específicos") se enlistan los estándares internacionales más importantes para sectores y actividades específicas, como el sector energético o el teletrabajo, mientras que el Anexo 4 ("Marcos de referencia internacionales relacionados a la ciberseguridad y que son relevantes") brinda un panorama de los marcos de referencia y guías de ciberseguridad a nivel internacional que complementan la información técnica sobre distintos procesos en la gestión de la ciberseguridad que se encuentra en los diferentes estándares internacionales.

Visto que la ciberseguridad es una preocupación apremiante ante los desafíos de la era digital y de la Industria 4.0, la adopción de estándares internacionales con sus conceptos básicos sólidos, herramientas de protección y prácticas de ciberseguridad industrial es fundamental para mantener seguras a las empresas y a las cadenas globales de valor.

2. ¿Qué son los estándares internacionales y cómo me ayudan a mejorar la ciberseguridad en mi empresa?

¿Qué son los estándares internacionales?[1]

// Son normas técnicas, de calidad o de gestión que se establecen a nivel global y que son reconocidas y utilizadas por organizaciones, industrias y países de todo el mundo. Estos estándares son desarrollados por organizaciones internacionales de normalización, como la Organización Internacional de Normalización (conocida como ISO, por sus siglas en inglés), la Comisión Electrotécnica Internacional (IEC, por sus siglas en inglés) y la Unión Internacional de Telecomunicaciones (UIT), entre otras.

En términos generales, los estándares internacionales proporcionan lineamientos y requisitos para realizar actividades específicas, como la gestión de calidad, la seguridad de la información, la gestión ambiental, la gestión de riesgos, entre otros. Además, son elaborados por expertos de diferentes países y se basan en el consenso y la experiencia colectiva de la comunidad internacional.

Una de sus características fundamentales es que su cumplimiento es voluntario. Esto significa que las organizaciones pueden adoptarlos y aplicarlos de manera opcional para mejorar sus procesos y productos o, en algunos casos, pueden ser requeridos por regulaciones o contratos.

Entre sus múltiples beneficios se encuentran la mejora de la calidad y la seguridad de productos y servicios, la facilitación del comercio internacional al establecer requisitos comunes, el impulso a la interoperabilidad y la compatibilidad entre diferentes sistemas y tecnologías, así como la promoción de buenas prácticas.

© YuriArcursPeopleimages/Freepik

Además de los estándares internacionales existen otros nacionales o regionales, que son reconocidos en contextos delimitados y son desarrollados por organismos de estandarización a nivel nacional. Sin embargo, cada vez más países buscan alinear sus estándares nacionales a los estándares internacionales para aprovechar los beneficios de estos últimos y evitar las ineficiencias que puedan surgir en mercados con presencia de estándares divergentes de distintos países. En México, los estándares nacionales son las Normas Mexicanas (NMX) que, al igual que los estándares internacionales, son de cumplimiento voluntario y son elaboradas y emitidas tanto por Secretarías, como por organismos privados de estandarización.

¿Qué beneficios puede traer la adherencia a estándares internacionales a mi empresa?

Cumplir con estándares internacionales en ciberseguridad, como por ejemplo ISO/IEC 27001, es especialmente importante para las PyMEs por las siguientes razones:

Gráfico 1. Beneficios para las empresas derivados de la adherencia a estándares internacionales de ciberseguridad. Elaboración propia.

¿Cómo puedo utilizar los estándares internacionales?

Existen distintas formas por medio de las cuales las empresas pueden utilizar los estándares internacionales. Por un lado, son portadores de tecnología y conocimiento ya que, al ser documentos que contienen lineamientos y herramientas para las soluciones técnicas, pueden servir como insumos para desarrollar e implementar nuevos procesos en una empresa; por ejemplo, para un nuevo proceso de gestión de riesgos en materia de ciberseguridad.

Para tener acceso a los contenidos técnicos de los estándares internacionales y utilizarlos como insumos y guías sólo se requiere adquirir una copia del estándar internacional correspondiente en las páginas web de la ISO o la IEC. Gracias a su costo moderado –una copia de ISO/IEC 27001 cuesta alrededor de $2,400.00 MXN (ISO, 2019)–, resultan también accesibles para PyMEs.

Sin embargo, para usar los estándares como insumos técnicos se requiere que el capital humano correspondiente dentro de la empresa comprenda, traduzca e implemente los lineamientos relevantes con base al contexto particular de la empresa.

Otra forma de utilizar los estándares internacionales es mediante la certificación. Además de asegurar que los lineamientos y procesos definidos en los estándares estén correctamente implementados en la empresa, la certificación sirve para generar confianza en clientes potenciales, en especial en empresas transnacionales. A través de este proceso, una tercera parte independiente y competente avala que la empresa esté implementando de manera efectiva los procesos y sistemas de gestión tal como lo prescribe el estándar.

Con frecuencia las empresas transnacionales ya piden certificaciones en estándares de sistemas de control de la calidad (ISO 9001), de gestión de la información (ISO 27001) o de gestión ambiental (ISO 14001).
En estos casos, aún sin ser de carácter legal u obligatorio, la certificación se convierte en un requisito para todos aquellos que buscan integrarse a cadenas globales de valor. Sin embargo, al involucrar auditorías externas por parte de organismos de certificación, este proceso se vuelve considerablemente más costoso. Los costos dependen de varios factores, incluyendo la complejidad y el tamaño de la empresa; por ejemplo, las certificaciones de las normas ISO pueden ir de los $50,000.00 a los $85,000.00 MXN anuales (ISO Update, 2020). Pero, al ser en muchos casos un requisito para la exportación a mercados como los Estados Unidos y la Unión Europea, ésta puede ser una inversión muy redituable o incluso necesaria, dependiendo del sector.

En el siguiente gráfico se muestran los pasos a seguir para que una organización pueda certificarse en un estándar internacional.

Gráfico 2. Pasos a seguir para la certificación en un estándar internacional. Elaboración propia.

3. Estándares internacionales y marcos de referencia en materia de ciberseguridad

3.1 Estándares internacionales de ciberseguridad

// Entre los estándares enfocados en ciberseguridad destacan las familias ISO 27000 e IEC 62443. La familia ISO 27000 es la referencia a nivel global en materia de seguridad en tecnologías de la información (TI), mientras que la serie IEC 62443 es fundamental para la gestión de la seguridad en tecnologías operativas (TO).

© Who is Danny/Freepik

Las tecnologías de la información se caracterizan por la aplicación de equipos de telecomunicación para tratar datos. Los sistemas TI corporativos se ocupan de los sistemas y el software del "negocio", como ERP, bases de datos de clientes, programas de contaduría, entre otros. En cambio, las tecnologías operativas están dedicadas a detectar y cambiar los procesos físicos a través de la monitorización y el control de dispositivos, también físicos. Incluyen, entre otros, a los sistemas de control industriales (ICS, por sus siglas en inglés) que comprenden los dispositivos, las redes y el software relacionados con la monitorización y el control de los procesos industriales. También se utilizan en otros ámbitos, como el suministro de energía, los dispositivos médicos, la automatización de edificios, las energías renovables o los ferrocarriles.

En este sentido, las empresas que cuenten con sistemas TI se deben guiar por los lineamientos definidos en los estándares de la serie ISO 27000, mientras que las empresas que utilizan tanto TI como TO se deben guiar por ambas series: ISO 27000 e IEC 62443.

La familia ISO 27000 consiste en más de 50 estándares que proporcionan lineamientos para la implementación de tecnologías y procesos de ciberseguridad, desde procesos fundamentales para cualquier organización –como la gestión de riesgos o gestión de incidentes– hasta aplicaciones específicas, como el Internet de las Cosas (IoT) o incluso ciudades inteligentes. Juntos, estos estándares permiten a organizaciones de todos los sectores y tamaños gestionar la seguridad de sus activos, como son la información financiera, la propiedad intelectual, los datos de los empleados y la información confiada por terceros. El principal estándar de esta serie, que sienta las bases para poder integrar los lineamientos definidos en los demás estándares de la familia, es ISO/IEC 27001:2022.

ISO/IEC 27001:2022. Seguridad de la información, ciberseguridad y protección de la privacidad establece los requisitos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) en una organización. Su objetivo es garantizar la confidencialidad, integridad y disponibilidad de la información, así como la gestión de los riesgos relacionados con la seguridad de la información. Para lograrlo, señala diferentes tipos de controles, mismos que se pueden apreciar en el gráfico 3.

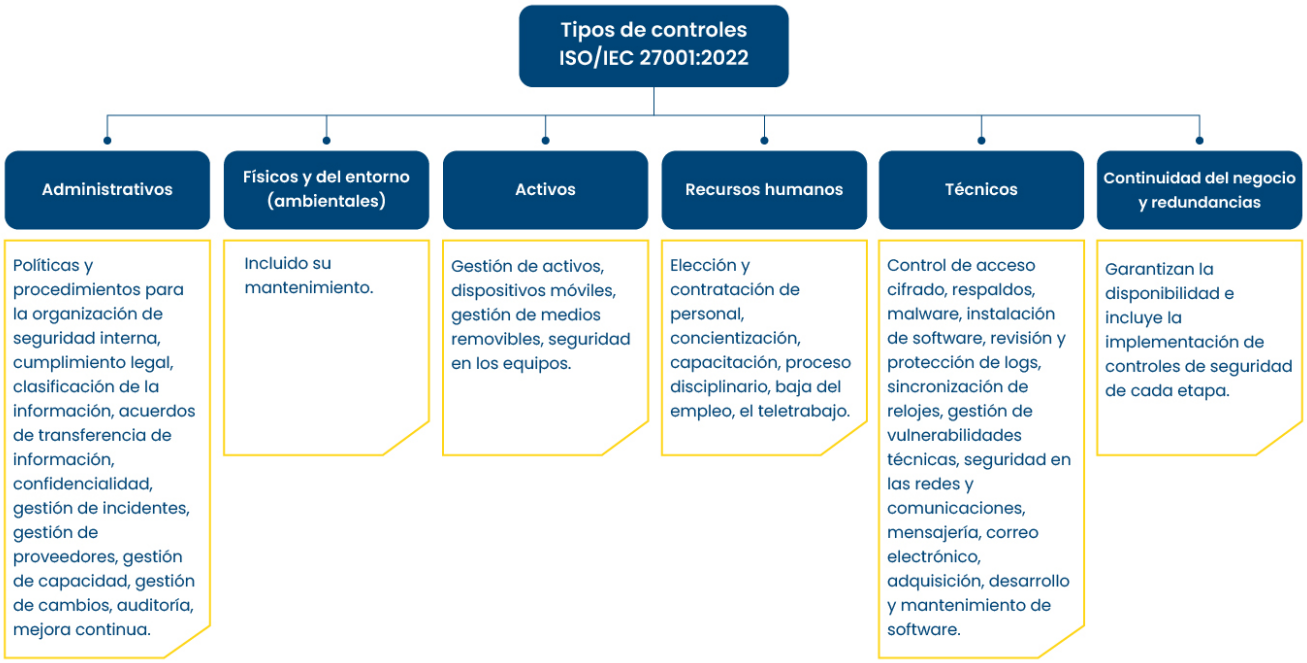

Gráfico 3. Tipos de controles (herramientas de protección) en el marco de ISO 27001. Elaboración propia.

El estándar ISO/IEC 27001 se basa en un enfoque de ciclo de vida del SGSI, que incluye su planificación, implementación, operación, monitoreo, revisión y mejora continua. Al implementarlo, las organizaciones deben identificar y evaluar los riesgos de seguridad de la información, establecer controles adecuados para mitigar estos riesgos, e instaurar un marco de políticas y procedimientos para garantizar la seguridad de la información en todos los niveles de la organización. Además, este estándar establece los requisitos para gestionar incidentes de seguridad, activos de información y proveedores, entre otros aspectos relacionados con la seguridad de la información.

El estándar ISO/IEC 27001 es quizás el más conocido por ser de aplicación general. Sin embargo, todos los detalles técnicos necesarios para los sectores específicos, como el de energía, salud, protección de datos, el Internet de las Cosas, etc., están disponibles en otras partes de la serie. Por ejemplo, ISO/IEC 27011 es relativa a la gestión de la seguridad para organizaciones de telecomunicaciones y se basa en ISO/IEC 27002.

Tanto ISO/IEC 27001 como ISO/IEC 27002 ya están adoptados como estándares nacionales en México, donde se conocen como NMX-I-27001-NYCE-2015 y NMX-I-27002-NYCE-2015.[2]

La serie de normas ISA/IEC 62443 define los requisitos y procesos para implementar y mantener sistemas de automatización y control industrial (IACS) electrónicamente seguros, adoptando un enfoque holístico que considera las perspectivas de operadores, integradores y fabricantes. Las normas ISA/IEC establecen puntos de referencia de ciberseguridad en todos los sectores industriales que utilizan IACS, como la automatización de edificios, la generación y distribución de energía eléctrica, los dispositivos médicos, el transporte y las industrias de procesos, como la química y la del petróleo y el gas. Actualmente incluye catorce estándares, informes técnicos (IT) y especificaciones técnicas (ET).

Dadas las diferentes prioridades en materia de ciberseguridad entre TI y TO, la serie ISA/IEC 62443 se centra principalmente en la mejora de la integridad y disponibilidad de los componentes

y sistemas. El cumplimiento de estas directrices busca fortalecer la seguridad de los procesos de producción y ayudar a identificar y abordar posibles vulnerabilidades. Esto puede reducir en gran medida el riesgo de que la información se vea comprometida o de que se produzcan paradas de producción. Al mismo tiempo, ISA/IEC 62443 brinda un enfoque holístico de la ciberseguridad, tendiendo un puente entre las operaciones y la tecnología de la información, así como entre la seguridad de los procesos productivos y la ciberseguridad.

Al igual que la serie ISO/IEC 27000, la serie ISA/IEC 62443 constituye una familia de estándares complementarios de ciberseguridad, en este caso enfocados en las tecnologías de operación. Esta familia se puede dividir en cuatro grupos principales, tal y como puede observarse en el gráfico 4.

En cuanto a la relación entre ISA/IEC 62443 e ISO/IEC 27000, si bien ambas difieren en su ámbito de aplicación individual –ISA/IEC 62443 se enfoca en TO e ISO/IEC 27000 en TI–no se deben entender como mutuamente excluyentes, sino como necesariamente complementarias para robustecer la ciberseguridad en empresas industriales. Mientras los estándares de la serie ISO/IEC 27000 brindan lineamientos para la protección de los sistemas de gestión de la información, se tienen que considerar las prácticas definidas en ISA/IEC 62443 para fortalecer la seguridad de los procesos de automatización.

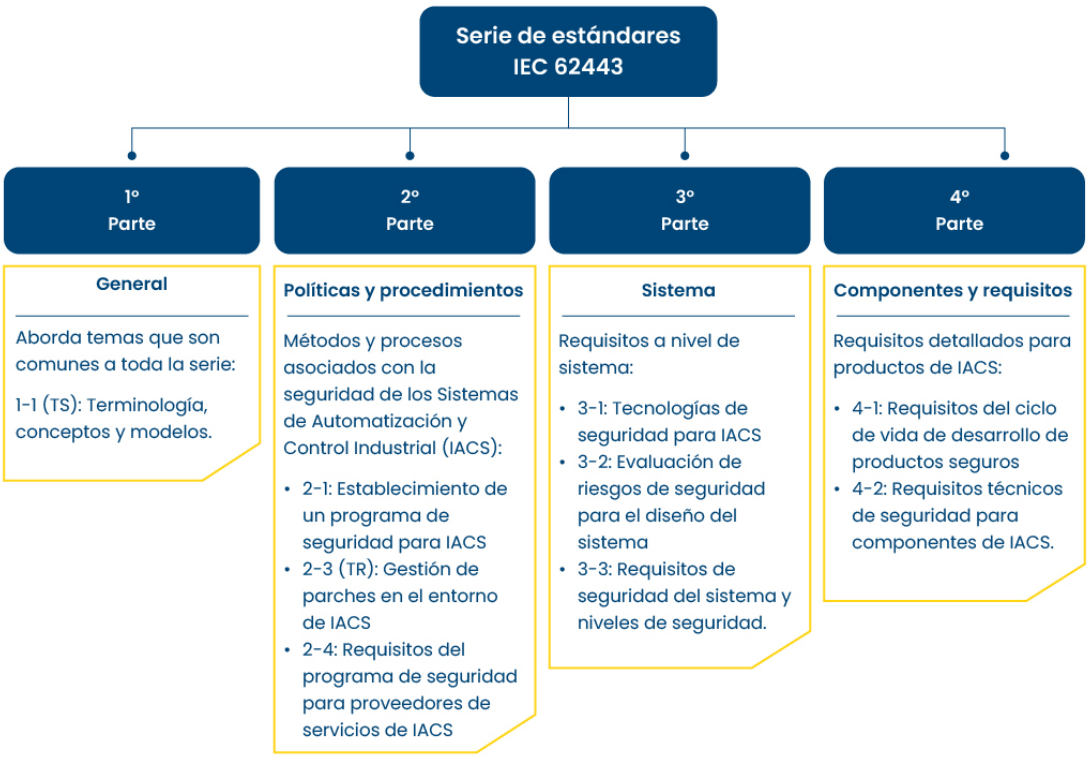

Gráfico 4. Los componentes de la serie IEC 62443.

3.2. Marcos de referencia de ciberseguridad

Para complementar los estándares también existen marcos de referencia internacionales y nacionales en materia de ciberseguridad. Los marcos de referencia son un conjunto de guías que contienen tanto estándares como prácticas para el control de daños, fortaleciendo las metodologías de seguridad de las organizaciones. Al igual que los estándares internacionales, están enfocados en proteger los sistemas de información para reducir las vulnerabilidades que podrían exponer a las organizaciones a posibles ataques por parte de ciberdelincuentes.[3]

Uno de los marcos de referencia más importantes es el Cybersecurity Framework del Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST, por sus siglas en inglés). Este consiste en estándares, directrices y mejores prácticas que ayudan a las organizaciones a mejorar su gestión de riesgos de ciberseguridad, y proporciona un inventario de funciones que las organizaciones deben ejecutar en el marco de una estrategia de ciberseguridad, como son: identificar, proteger, detectar, responder y recuperar, entre otras.

Al mismo tiempo, ofrece un marco de referencia para que las organizaciones puedan conocer mejor su estado de madurez en ciberseguridad. Este comprende cuatro niveles, que inician en el nivel 1 (madurez parcial), donde la organización está familiarizada con el NIST CSF pero carece de los procesos y recursos para permitir la seguridad de la información, y llegan hasta el nivel 4 (adaptabilidad), en el que la organización ha alcanzado la ciber-resiliencia y existe un enfoque en toda la organización para la gestión de riesgos de seguridad de la información.

El NIST CSF contiene también una guía de implementación del marco de referencia, que abarca desde la definición de objetivos de una estrategia de ciberseguridad particular, hasta la elaboración de un plan de acción que incluya hitos cuantificables y los recursos disponibles (personas, presupuesto y tiempo). En contraste con los estándares internacionales, este marco de referencia es de dominio público y se puede encontrar haciendo clic aquí.

Por la relevancia que tienen a nivel internacional estos marcos de referencia, al final de los siguientes capítulos se mencionarán –adicionalmente a los estándares internacionales– aquellos que sean más importantes en la materia.

4. Mapeo de estándares internacionales de ciberseguridad por funciones y aplicaciones

4.1 Conceptos básicos de ciberseguridad – Estándares de definiciones

// En este capítulo se presentan aquellos estándares internacionales que contienen definiciones básicas en materia de ciberseguridad, los cuales servirán como fundamento para la comprensión de los lineamientos publicados en los demás estándares. Estas definiciones incluyen la diferencia entre ciberseguridad y seguridad de la información, y abarcan un conjunto de prácticas y medidas diseñadas para proteger los sistemas informáticos, la identificación y clasificación de la información personal, así como la confidencialidad, integridad y disponibilidad de la información, que son los pilares fundamentales de la ciberseguridad. Entre los estándares claves de definiciones se encuentran: ISO/IEC 27000, ISO/IEC 27033-1, ISO/IEC 27034-1, e ISO/IEC 27036-1.

ISO/IEC 27000:2018. Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información – Visión general y vocabulario[4]

ISO/IEC 27000:2018 proporciona una visión general sobre los sistemas de gestión de la seguridad de la información (SGSI), y los términos y definiciones utilizados en la familia de estándares ISO/IEC 27000. Todos los estándares de la serie hacen referencia a las definiciones contenidas en ISO/IEC 27000. Este documento es aplicable a todos los tipos y tamaños de organización (por ejemplo: empresas comerciales, agencias gubernamentales y organizaciones sin fines de lucro).

© ThapanOnphalai /Freepik

ISO/IEC 27034-1:2011. Tecnología de la información – Técnicas de seguridad – Seguridad de las aplicaciones – Parte 1: Visión general y conceptos[5]

ISO/IEC 27034 brinda orientación para ayudar a las organizaciones a integrar la seguridad en los procesos utilizados para la gestión de sus aplicaciones. ISO/IEC 27034-1:2011 presenta una visión general de la seguridad de las aplicaciones, e introduce definiciones, conceptos, principios y procesos implicados en la seguridad de las mismas.

ISO/IEC 27036-1:2021. Ciberseguridad – Relaciones con los proveedores – Parte 1: Visión general y conceptos[6]

Este documento es una parte introductoria del estándar ISO/IEC 27036.
Proporciona una visión general y orientación a las organizaciones para ayudar a proteger su información y sistemas de información en el contexto de las relaciones con los proveedores. También introduce conceptos que se describen a detalle en otras partes de la norma ISO/IEC 27036. De igual forma, aborda las perspectivas tanto de los adquirentes, como de los proveedores.

4.2 Estándares de gestión de riesgos

La gestión de riesgos es el proceso fundamental para una adecuada implementación de una estrategia de ciberseguridad; es lo que permite a las empresas identificar, evaluar y tratar los riesgos en materia de ciberseguridad y seguridad de la información. Tiene como objetivo reducir y controlar su impacto en la autenticidad, el no repudio, la confidencialidad, la disponibilidad e integridad de la información, los activos tecnológicos y los servicios que soportan al negocio.

Sin una correcta gestión de riesgos, no vamos a ser conscientes de las "puertas traseras" y debilidades que existen en nuestros sistemas TI y su entorno, ni vamos a poder anticipar hacia dónde se pudieran dirigir los posibles ataques. El proceso de gestión de riesgos es el primer paso para analizar nuestro entorno como empresa y los riesgos que conlleva y, una vez que estos sean identificados, analizados y evaluados, generar un plan de tratamiento a partir de diferentes estrategias como el mitigar, evitar y combatir, entre otras. Para aprender a más detalle cómo establecer un proceso de gestión de riesgos para tu empresa paso a paso, consulta la "Guía de implementación de medidas de ciberseguridad para empresas" que forma parte de esta serie de publicaciones.

El caso del ciberataque a una cadena de hoteles en 2014 muestra de forma impactante las consecuencias económicas que puede tener una gestión de riesgos inadecuada.

Caso 1. El ataque a una cadena internacional de hoteles (2014)

En 2014, una cadena internacional de hoteles fue víctima de un ciberataque que le permitió acceder a los ciberdelincuentes a los datos personales de 339 millones de huéspedes de la cadena, incluyendo sus pasaportes, información de contacto e información financiera.

Esta filtración de datos fue posible debido a los fallos en ciberseguridad de la compañía, que indican un proceso deficiente de gestión de riesgos. Una investigación del organismo británico de control de la privacidad de datos, la Oficina del Comisionado de Información (ICO), demostró que la empresa no había adoptado las medidas técnicas u organizativas adecuadas para proteger los datos personales tratados en sus sistemas, tal como lo exigía la ley del país. Por ejemplo, se detectó que, aunque los números de las tarjetas de crédito se almacenaban cifrados, las claves de cifrado se guardaban en el mismo servidor, lo cual facilitó el acceso de los atacantes; lo mismo ocurría con los números de pasaporte.

Como consecuencia de esta infracción legal, se multó a la cadena hotelera con 18,4 millones de libras.

Para evitar este tipo de experiencias desagradables, se pueden implementar diversos estándares internacionales que reúnen lineamientos para el desarrollo de un proceso de gestión de riesgos robusto y completo, y que sirvan para identificar vulnerabilidades en los sistemas y tomar medidas adecuadas. Entre estos destacan: NMX-I-27005-NYCE-2019, que se basa en ISO 27001 e ISO/IEC 27005:2022, que es la versión actualizada de este; ISO/IEC 31000; ISO/IEC 27557; ISO/IEC 31010; así como el marco de referencia Risk Management Framework (RMF) del NIST.

NMX-I-27005-NYCE-2019 | ISO/IEC 27005:2018. Tecnologías de la información –Técnicas de seguridad – Gestión de riesgos en seguridad de la información[7,8]

Este estándar proporciona las directrices para la gestión de riesgos en materia de seguridad de la información. Apoya los conceptos generales especificados en NMX-I-27001-NYCE-2015, basada a su vez en ISO/IEC 27005:2018, y está diseñado para ayudar a implementar medidas para mejorar la seguridad de la información basada en el enfoque de la gestión de riesgos. Para entender correctamente este estándar, es importante conocer los conceptos, modelos, procesos y terminologías descritas en NMX-I-27001-NYCE-2015 y en NMX-I-27002-NYCE-2015. Asimismo, este estándar puede aplicarse a todos los tipos de organizaciones (por ejemplo: empresas comerciales, dependencias gubernamentales, organizaciones sin fines de lucro) que buscan fortalecer sus procesos de gestión de riesgos y evitar aquellos que pueden comprometer la seguridad de la información de la organización.

Hemos de señalar que a nivel internacional se actualizó ISO/IEC 27005 en el año 2022. En la nueva versión ISO/IEC 27005:2022 se fortaleció su alineación con ISO/IEC 27001 e ISO 31000:2018, y se incluyeron nuevos conceptos, criterios y enfoques para la gestión de riesgos, como la evaluación continua y un enfoque de identificación de riesgos basado en eventos, contrastando con el enfoque basado en activos que ya formaba parte de ISO/IEC 27005:2018.

ISO/IEC 31000:2018. Gestión de riesgos – Lineamientos[9]

La norma ISO 31000:2018 engloba herramientas y procesos de gestión ante todos los tipos de riesgos a los que se puede enfrentar una organización. No es específica para riesgos de ciberseguridad, pero forma una base para la gestión de riesgos cibernéticos. Tampoco es específica para una industria o un sector, por lo que la aplicación de estas directrices puede adaptarse a cualquier organización y a su contexto específico.

Además, este estándar puede utilizarse durante toda la vida de la organización y puede aplicarse a cualquier actividad, incluida la toma de decisiones en todos los niveles.

ISO/IEC 27557:2022. Seguridad de la información, ciberseguridad y protección de la privacidad – Aplicación de la norma ISO 31000:2018 para la gestión del riesgo de privacidad organizacional[10]

Este documento proporciona directrices para gestionar el riesgo en materia de privacidad de la organización. Funciona como una especificación de las metodologías de gestión de riesgos definidas en la norma ISO 31000:2018 con el fin específico de salvaguardar la privacidad institucional. También ayuda a orientar a las organizaciones para poder integrar los riesgos relacionados con el procesamiento de la información de identificación personal (IIP) como parte de un programa de gestión de riesgos de privacidad organizacional.

Distingue entre el impacto que el procesamiento de IIP puede tener en un individuo y las consecuencias para las organizaciones (por ejemplo: daño a la reputación), y brinda orientación para incorporar lo siguiente en la evaluación general de riesgos de la organización:

- Consecuencias organizativas de los impactos adversos sobre la privacidad de los individuos.

- Consecuencias organizativas de los sucesos relacionados con la privacidad que perjudican a la organización (como daños a su reputación), sin causar ningún impacto adverso sobre la privacidad de los individuos.

Este estándar ayuda a establecer un programa de privacidad basado en el riesgo que puede integrarse en la gestión global de riesgos de la organización. También es aplicable a todo tipo y tamaño de organización que procese IIP o que desarrolle productos y servicios que puedan utilizarse para procesar IIP, incluidas empresas públicas y privadas, entidades gubernamentales y organizaciones sin ánimo de lucro.

ISO/IEC 31010:2019. Gestión de riesgos – Técnicas de evaluación de riesgos[11]

ISO/IEC 31010:2019 ayuda a orientar en la selección y aplicación de técnicas para evaluar un riesgo en una amplia gama de situaciones. Estas técnicas se utilizan para facilitar la toma de decisiones cuando hay incertidumbre, proporcionar información sobre riesgos particulares, y como parte de un proceso de gestión de riesgos. El documento ofrece resúmenes de una serie de 31 técnicas para el análisis de riesgos, como son: análisis de peligros y puntos de control críticos (APPCC), análisis de impactos en el negocio y árboles de decisión con referencias a otros documentos en los que las técnicas se describen con más detalle.

Marcos de referencia relevantes

NIST Risk Management Framework

Este Marco de Gestión de Riesgos (RMF, por sus siglas en inglés) del NIST proporciona un proceso sistemático de siete pasos que ayuda a las organizaciones a incorporar la seguridad, la privacidad y la gestión de riesgos de la cadena de suministro cibernética en el ciclo de vida del desarrollo de los sistemas. El RMF es resultado de la Iniciativa de Transformación de la Fuerza de Tarea Conjunta (JTF, por sus siglas en inglés) que incluye representantes del NIST, el Departamento de Defensa (DOD, por sus siglas en inglés), la Oficina de la Dirección de Inteligencia Nacional (ODNI, por sus siglas en inglés) y el Comité de Sistemas de Seguridad Nacional (CNSS, por sus siglas en inglés) de Estados Unidos. El RMF considera factores como la eficacia y cualquier restricción impuesta por leyes relevantes, directivas, órdenes ejecutivas, políticas, estándares o regulaciones. Su metodología se puede aplicar a organizaciones de todos los tamaños y sectores, así como a sistemas nuevos y existentes, independientemente de su tipo o tecnología (por ejemplo: IoT o sistemas de control).

A diferencia de los estándares internacionales, este documento es de dominio público y se puede encontrar aquí.

4.3 Estándares sobre controles y su implementación

Los controles de ciberseguridad son mecanismos utilizados para prevenir, detectar, corregir, compensar o disuadir las ciberamenazas y los ataques.[12] Los mecanismos van desde controles físicos –como guardias de seguridad y cámaras de vigilancia– o controles administrativos –como la definición de políticas y procedimientos–, hasta controles técnicos –como el software *antimalware*, el cifrado y la autenticación multifactor.

Hay muchas formas diferentes de aplicar los controles en función de la naturaleza de lo que se intenta proteger. Por ello, es importante primero contar con un inventario de activos y análisis de riesgos sólido, para identificar cuáles son los principales activos de la empresa que se buscan salvaguardar, y cuáles son las principales debilidades en su entorno y sus sistemas que pueden facilitar el acceso de personas no autorizadas.

En su conjunto, los controles apuntan a lo que se llama *"hardening"* de los ecosistemas de TI; esto es, una reducción de la superficie de ataque. La superficie de ataque está compuesta por todas las entradas, debilidades, defectos o puertas traseras en un sistema que pueden servir como rutas potenciales para un ciberataque.[13] El

hardening del sistema es un proceso continuo que se tiene que implementar en todo el ciclo de vida de las TI, contemplando su instalación, configuración y mantenimiento.

El caso 2 en el recuadro azul, que ejemplifica el ataque a un proveedorde servicios de nombres de dominio (DNS) en 2016, ilustra cómo la implementación de medidas concretas de *hardening* hubieran podido defender a la empresa contra el ataque sufrido.

En esta sección podemos apreciar los más importantes estándares internacionales que nos ayudan a conocer, seleccionar e implementar controles adecuados y así evitar situaciones como las relatadas en el Caso 2. Entre estos estándares y marcos de referencia destacan ISO/IEC 27002, ISO/IEC 27008, ISO/IEC 27004, ISO 27022, NIST 800-53 y COBIT 2019.

NMX-I-27002-NYCE-2015 | ISO/IEC 27002:2022. Seguridad de la información, ciberseguridad y protección de la privacidad – Controles de seguridad de la información[14]

Proporciona un conjunto de controles genéricos de seguridad de la información de referencia, que incluye una guía de orientación para la implementación de los controles mencionados en ISO/IEC 27001. La nueva versión contempla controles adicionales, tales como: seguridad en los servicios de la nube, inteligencia de amenazas, enmascaramiento de datos y gestión de configuración, entre otros. Incluye atributos y referencias que facilitan su alineación con los marcos internacionales de ciberseguridad.

ISO/IEC 27008:2019. Informática – Técnicas de seguridad – Directrices para la evaluación de los controles de seguridad de la información[15]

Este documento ofrece orientación sobre la revisión y evaluación de la implementación y el funcionamiento de los controles de seguridad de la información, incluyendo la evaluación técnica de los controles del sistema de información, de conformidad con los requisitos de seguridad de la información establecidos por una organización.
Es una guía para saber cómo revisar y evaluar los controles de seguridad de la información que se gestionan a través de un sistema de gestión de seguridad de la información (SGSI) especificado por ISO/IEC 27001.

Es aplicable a todo tipo y tamaño de organizaciones que lleven a cabo revisiones de seguridad de la información y comprobaciones de conformidad técnica.

Caso 2. Ataque a un proveedor de servicios de redirección de nombres de dominio (2016)

Este incidente consistió en un ataque de denegación de servicio distribuido (DDoS) dirigido a la infraestructura de la empresa, afectando la accesibilidad a numerosos sitios web y servicios en línea.

Durante el ataque, se utilizó una *botnet* masiva compuesta por dispositivos IoT comprometidos para inundar los servidores de la compañía con un gran volumen de solicitudes de tráfico. Esta sobrecarga de tráfico abrumó los servidores, lo que resultó en la interrupción de sus servicios. Como resultado, muchos sitios web y servicios que dependían de la infraestructura de este proveedor experimentaron una interrupción en su accesibilidad, lo que afectó negativamente a los usuarios y a las organizaciones.

Este incidente subrayó la necesidad de implementar controles de seguridad sólidos en dispositivos IoT y de proteger los sistemas contra ataques DDoS a través de la prevención con planes de contingencia y de recuperación ante desastres para minimizar el impacto de futuros ataques similares.

ISO/IEC TS 27022:2021. Tecnología de la información – Orientación sobre los procesos del sistema de gestión de la seguridad de la información[16]

Este documento define un modelo de referencia de rendimiento (PRM) para la gestión de la seguridad de la información, que cumple con los criterios definidos en la norma ISO/IEC 33004 para los modelos de referencia de procesos. Su objetivo es guiar a los usuarios de ISO/IEC 27001 para incorporar el enfoque de procesos descrito por ISO/IEC 27000:2018, apartado 4.3, dentro del SGSI, además de estar alineado con todo el trabajo realizado dentro de otras normas de la familia ISO/IEC 27000 desde la perspectiva de la operación de los procesos del SGSI, y apoyar a los usuarios en la operación de un SGSI.

ISO/IEC 27033-1:2015. Tecnología de la información – Técnicas de seguridad – Seguridad de red – Parte 1: Visión general y conceptos[17]

ISO/IEC 27033-1:2015 define y describe los conceptos asociados a la seguridad de la red y proporciona orientación para su gestión, así como una visión general de la seguridad de la red y las definiciones relacionadas.

Es relevante para cualquiera que participe en la propiedad, el funcionamiento o el uso de una red. Esto incluye a los altos directivos y otros gestores o usuarios no técnicos, además de los gestores y administradores que tienen responsabilidades específicas en la seguridad de la información y/o la seguridad de la red, el funcionamiento de la red, o que son responsables del programa general de seguridad de una organización y del desarrollo de la política de seguridad. También resulta crucial para cualquier persona involucrada en la planificación, diseño e implementación de los aspectos arquitectónicos de la seguridad de la red.

De igual manera, ISO/IEC 27033-1:2015 incluye lo siguiente:

- Orientación sobre cómo identificar y analizar los riesgos de seguridad de la red y la definición de los requisitos de seguridad de la red basados en ese análisis.
- Visión general de los controles que sustentan las arquitecturas técnicas de seguridad de las redes y los controles técnicos relacionados, así como de los controles no técnicos y los controles técnicos que no sólo son aplicables a las redes.
- Información sobre cómo lograr arquitecturas de seguridad técnica de red de buena calidad, y los aspectos de riesgo, diseño y control asociados con escenarios de red típicos y áreas de "tecnología" de red (que se tratan en detalle en partes posteriores de ISO/IEC 27033), y aborda brevemente las cuestiones asociadas con la implementación y el funcionamiento de los controles de seguridad de red y la supervisión y revisión continuas de su implementación.

En general, brinda una visión general de esta norma internacional y una "hoja de ruta" hacia todas las demás partes.

ISO/IEC 27004:2016. Tecnología de la información – Técnicas de seguridad – Gestión de la seguridad de la información – Seguimiento, medición, análisis y evaluación[18]

La norma ISO/IEC 27004:2016 proporciona directrices destinadas a ayudar a las organizaciones a evaluar el desempeño de la seguridad de la información y la eficacia de su sistema de gestión de la seguridad de la información con el fin de cumplir con los requisitos de la norma ISO/IEC 27001:2013, apartado 9.1. También establece el seguimiento y la medición del desempeño de la seguridad de la información, así como el seguimiento y la medición de la eficacia de un sistema de gestión de la protección de la información (SGSI), incluyendo sus procesos y controles.

Marcos de referencia relevantes

COBIT 2019: Con área de enfoque en seguridad de la información

Esta es la versión más reciente del modelo "Objetivos de control para **el gobierno y la gestión de Tecnologías de la Información** y Tecnologías Relacionadas" (COBIT, por sus siglas en inglés). Es un marco de referencia que proporciona orientación para auditar la gestión y controlar los sistemas de información dentro de una empresa. Maneja un enfoque holístico, esto es, contempla todos los aspectos de una organización, como lo son: su estructura organizacional, sus políticas y procedimientos, su infraestructura, entre otros. Si bien COBIT nació como una guía para auditores, hoy en día se ha convertido en una referencia para diversas partes interesadas, que pueden ir desde la Junta Directiva de una empresa hasta el Departamento de Recursos Humanos.

NIST SP 800-53B. Líneas base de control para sistemas de información y organizaciones

En inglés llamada "Control Baselines for Information Systems and Organizations", es una publicación especial elaborada por el Grupo de Trabajo de la Fuerza de Tarea Conjunta Interinstitucional del NIST. Dentro del documento se pone a disposición de agencias federales y organizaciones del sector privado múltiples lineamientos para mantener medidas de seguridad y privacidad en los sistemas de información en todo tipo de plataformas informáticas, incluyendo sistemas de propósito general, sistemas ciberfísicos, sistemas basados en la nube, dispositivos móviles y sistemas de control industrial y de procesos. Se incluyen recomendaciones sobre controles de acceso, concientización y capacitación del personal, evaluación de medidas, autorización y seguimiento, gestión de configuración, protección física y del entorno, entre otros.

© Ar_fp/Freepik

4.4 Estándares internacionales para aplicaciones en la nube

Una de las herramientas de trabajo en el ámbito digital que se ha ido expandiendo y es utilizada por cada vez más empresas es la prestación de servicios en la nube. Estos ofrecen extensos beneficios debido al dinamismo y la flexibilidad que brindan a las empresas con respecto a los requerimientos de compra y aprovisionamiento de hardware. Adicionalmente, los servicios de nube minimizan el tiempo de inactividad y permiten reducir costos.

La nube también ofrece algunos beneficios de seguridad. Sin embargo, estos beneficios sólo son aplicables si se comprenden y adoptan modelos nativos de la nube y se acondicionan las arquitecturas y controles para ajustarse con los atributos y las condiciones de las plataformas en la nube.

De igual forma, es importante seleccionar nubes que cuenten con altos niveles de protección, como nos muestra este caso de ciberataques a embajadas en Portugal y Brasil.

Caso 3. Ciberataques a embajadas en Portugal y Brasil a través de su servicio de nube (2022)

En mayo y junio de 2022 un grupo de ciberdelincuentes lanzó una serie de ataques a través de sistemas de almacenamiento basados en la nube para atacar varias misiones diplomáticas.

Las campañas se dirigieron a embajadas en Brasil y Portugal utilizando documentos de *phishing* con un enlace a un archivo HTML malicioso, que servía de gotero para otras cargas útiles maliciosas, como reveló una investigación de la Unidad 42 de Palo Alto Networks. Según los investigadores, los datos recopilados durante estas campañas incluyen nombres de máquinas, nombres de usuario y una lista de procesos en ejecución.

Los expertos también indicaron que el uso de servicios en la nube representa una manera económica de utilizar aplicaciones confiables, dado que los atacantes cibernéticos pueden obtener cuentas de manera sencilla y gratuita, empleándolas para recopilar información y alojar software malicioso.

Los estándares ISO/IEC 27017 e ISO/IEC 27018 contienen información valiosa para evitar este tipo de incidentes. De hecho, ISO/IEC 27017 señala buenas prácticas para la implementación de controles de seguridad en la nube, tanto desde la perspectiva de los prestadores como de los usuarios del servicio; mientras que ISO/IEC 27018 especifica los lineamientos para la protección de la información de identificación personal.

ISO/IEC 27017:2015. Tecnología de la información – Técnicas de seguridad – Código de buenas prácticas para los controles de seguridad de la información basados en la norma ISO/IEC 27002 para servicios en la nube[19]

Esta norma proporciona directrices para los controles de seguridad y una guía de implementación, tanto para proveedores de servicios en la nube, como para clientes de servicios en la nube, brindando:

- Orientación adicional para la implementación de los controles pertinentes especificados en ISO/IEC 27002.
- Controles adicionales con una guía de implementación que se refieren específicamente a los servicios en la nube.

ISO/IEC 27018:2019. Tecnología de la información – Técnicas de seguridad – Código de prácticas para la protección de la información de identificación personal (IIP) en nubes públicas que actúan como procesadores de IIP[20]

Este documento establece los objetivos de control comúnmente aceptados, así como controles y directrices para implementar medidas de protección de la información de identificación personal (IIP), en línea con los principios de privacidad de la norma ISO/IEC 29100 para el entorno de computación en nube pública.

En particular, especifica las directrices basadas en la norma ISO/IEC 27002, teniendo en cuenta los requisitos reglamentarios para la protección de la IIP que pueden ser aplicables en el contexto del entorno o en entornos de riesgo para la seguridad de la información de un proveedor de servicios de nube pública.

4.5 Estándares para Tecnologías de Operación

La ciberseguridad en el ámbito industrial se ha convertido en un tema de gran importancia en los últimos años debido a la creciente conectividad de los dispositivos y los sistemas industriales.

Con el aumento del uso de dispositivos del Internet Industrial de las Cosas (IIoT, por sus siglas en inglés) y los Sistemas de Control Industrial (ICS, por sus siglas en inglés), los riesgos de seguridad cibernética se han multiplicado.

El IIoT es un subconjunto de la IoT que hace referencia a la tecnología IoT utilizada en los procesos de manufactura. Se trata de una tecnología crucial en la Industria 4.0. Puede tener muchos de los mismos usos y beneficios que la IoT, sólo que el nivel de especialización y las características de construcción y operación de los dispositivos son mucho más robustos. Puede integrar sensores inteligentes en maquinaria de fabricación, sistemas de energía e infraestructuras como tuberías y cableado. Estos sensores, a través de los datos que recopilan y su funcionalidad avanzada, ayudan a las empresas industriales a aumentar su eficiencia, productividad, la seguridad de los empleados y mucho más.

Por otro lado, los sistemas de automatización y control industrial (IACS) son utilizados para controlar y monitorear los procesos industriales. Estos sistemas incluyen controladores lógicos programables (PLC, por sus siglas en inglés), sistemas de control de procesos (DCS, por sus siglas en inglés) y sistemas de supervisión y control de procesos a distancia (mejor conocidos en inglés como SCADA). Al igual que los dispositivos IoT, estos sistemas también son vulnerables a ataques cibernéticos debido a su conectividad a internet.

Las consecuencias de un ciberataque exitoso contra un IACS o una red de dispositivos IIoT son esencialmente diferentes a las de un ataque a los sistemas de información. Mientras que

© User2846165/Freepik

las principales secuelas de un ciberataque contra sistemas informáticos es la pérdida de privacidad debido a la divulgación de la información, las consecuencias para un sistema de control industrial pueden incluir daños a la integridad del producto, al medioambiente o, incluso, poner en peligro la salud y la vida de trabajadores y de la población.

El caso del ciberataque a la planta de tratamiento de agua en Oldsmar, Florida, ilustra los peligros particulares que surgen en el caso de los ciberataques a tecnologías operativas (TO), a diferencia de los ataques a la tecnología de la información (TI), y cómo el implementar los controles para proteger las TO que se recomiendan en la serie ISA/IEC 62443 puede ayudar a evitar daños a infraestructuras críticas, e incluso a la salud y la vida de las personas.

Caso 4. Ataque a la planta de tratamiento de agua en Oldsmar, Florida (2021)

En febrero de 2021 ocurrió un ataque cibernético a una planta de tratamiento de agua en Oldsmar, Florida, que se destacó por su gravedad. Durante el mismo, un pirata informático accedió al sistema de control de la planta y aumentó de manera peligrosa la cantidad de hidróxido de sodio (lejía) en el agua potable. Esta acción pudo haber tenido consecuencias devastadoras para la salud pública y el suministro de agua si no se hubiera detectado a tiempo.

Afortunadamente, el ataque fue frustrado debido a varios factores: en primer lugar, el equipo de la planta de tratamiento pudo detectar el acceso no autorizado mientras ocurría y revertir con rapidez los cambios realizados por el intruso. En segundo, la seguridad del sistema presentaba ciertas limitaciones, como el hecho de que el controlador de la planta no estaba conectado directamente a internet y requería de una conexión VPN para acceder a él.

Este incidente resalta la importancia de contar con medidas sólidas de seguridad cibernética en infraestructuras críticas como plantas de tratamiento de agua, y las consecuencias graves que ciberataques a redes industriales pudieran a llegar a tener.

Debido a que existen diferentes riesgos, las prioridades en materia de ciberseguridad en los sistemas de control industrial son distintas. Las priorizaciones de los elementos de la triada de ciberseguridad –que son la confidencialidad, la integridad y la disponibilidad de la información y los sistemas– son opuestas para las tecnologías de la información y las tecnologías de operación, a las que pertenecen los IACS y el IIoT.

Así, los sistemas TI dan prioridad a la confidencialidad de los datos por encima de otros elementos de la triada de ciberseguridad, como se ilustra en el siguiente gráfico.

Gráfico 5. Priorización de principios de seguridad para Tecnologías de Información (IT, por sus siglas en inglés) y Tecnologías de Operación (OT, por sus siglas en inglés)

Por ejemplo, si durante un tiempo no puedo acceder a mis estados financieros mediante el software que utiliza la empresa (disponibilidad), esto puede causar un daño, pero es probable que el daño fuese mucho mayor si estos estados financieros llegaran a publicarse (confidencialidad). En contraste, los sistemas TO ponen por delante la disponibilidad de su tecnología, dado que una limitación de esta –digamos, por un paro de las máquinas en la planta– afectaría directamente a la producción y, por ende, tendría consecuencias económicas. Esta priorización inversa entre los principios de seguridad desde una perspectiva TI/TO es un reto importante para la convergencia TI/TO.

Como hemos visto antes, la serie más importante de estándares internacionales de ciberseguridad para las Tecnologías de Operación es la ISA/IEC 62443. En esta sección profundizaremos un poco más en ciertas partes de dicha serie.

ISA/IEC 62443-2-1-2009. Seguridad para sistemas de control y automatización industrial – Parte 2-1: Establecimiento de un programa de seguridad para sistemas de automatización y control industrial[21]

Este estándar define los elementos necesarios para establecer un sistema de gestión de la

ciberseguridad (SGC) para sistemas de control y automatización industrial (IACS, por sus siglas en inglés), y proporciona orientación sobre cómo desarrollar estos elementos.

Dichos elementos descritos en este documento están relacionados principalmente con la política, los procedimientos, las prácticas y el personal, y describen qué debe incluirse en el SGC definitivo de una organización.

ISA/IEC 62443-2-2. Seguridad para sistemas de control y automatización industrial – Parte 2-2: Niveles de protección de IACS

Este estándar especifica una metodología para evaluar la protección de los sistemas IACS en funcionamiento. Abarca tanto la evaluación de las medidas de seguridad organizativas como técnicas. Su objetivo es proporcionar un método coherente y reproducible para evaluar la protección del SGC en funcionamiento, con base en una estrategia de defensa a profundidad. Se subraya que el desarrollo, funcionamiento y mantenimiento de un sistema de protección holístico requiere la participación de los operadores, los proveedores de servicios para la integración y el mantenimiento, así como los proveedores de servicios del SGC.

ISA/IEC 62443-2-5. Seguridad para sistemas de control y automatización industrial – Parte 2-5: Guías de implementación para los propietarios de activos del SGC

Esta parte de la serie proporciona orientación sobre lo que se requiere para operar un sistema eficaz de gestión de la ciberseguridad en un SGC. Los destinatarios son los usuarios finales y los propietarios de activos responsables del funcionamiento de dicho programa.

ISA/IEC 62443-3-1:2009. Redes de comunicación industriales – Seguridad de redes y sistemas – Parte 3-1: Tecnologías de seguridad para sistemas de control y automatización industrial[22]

Esta sección de la serie brinda una evaluación actual de diversas herramientas de ciberseguridad, mitigación en ciberseguridad, contramedidas de mitigación y tecnologías que pueden aplicarse a diversas industrias. Incluye varias categorías de tecnologías de ciberseguridad centradas en los sistemas de control, los tipos de productos disponibles en esas categorías, así como los pros y los contras de utilizar esos productos en los entornos IACS automatizados en relación con las amenazas previstas y las vulnerabilidades cibernéticas conocidas.

4.6 Estándares de gestión de incidentes

A pesar de todas las medidas de prevención que podemos implementar, nunca se puede eliminar por completo el riesgo de un incidente de seguridad de la información. Este se da cuando uno o múltiples eventos de seguridad de la información o de ciberseguridad otorgan acceso a una persona o grupo de personas no acreditadas a la información almacenada en dispositivos físicos o virtuales.

Afrontar un incidente de seguridad de la información o de ciberseguridad de manera efectiva es una tarea compleja que requiere de una planeación previa y exhaustiva, una revisión y actualización constantes, así como del apoyo de todas las áreas que conforman una organización, como son: recursos humanos, sistemas, administración y finanzas, legal y marketing, entre otras.

En el siguiente caso de un ciberataque se puede apreciar cómo el estar preparado para un incidente de ciberseguridad puede ayudar a mitigar significativamente los daños en el momento de un ataque.

Caso 5. El ataque de WannaCry a una empresa de telecomunicaciones (2017)

En mayo de 2017, una empresa española de telecomunicaciones fue víctima del *ransomware* WannaCry, con lo cual pasó a formar parte de una campaña global contra este virus que afectó a miles de organizaciones en todo el mundo. En el caso específico de esta empresa, WannaCry infectó una parte de su red y sistemas, causando interrupciones y afectando la operatividad de varios de sus servicios.

En este incidente se pueden observar varios elementos de la gestión de incidentes que fueron aplicados por la compañía para hacer frente al ataque:

- Detección temprana: la empresa detectó con rapidez la infección y la propagación del *ransomware* en su red. La identificación temprana del incidente fue esencial para poder responder de manera oportuna y evitar que el ataque se propagara aún más.
- Respuesta rápida: la compañía activó de inmediato su equipo de respuesta a incidentes de seguridad para contener la situación y mitigar los efectos del ataque. Su veloz respuesta ayudó a minimizar el impacto y a limitar la cantidad de sistemas y datos comprometidos.
- Comunicación interna y externa: durante el incidente, la empresa estableció una comunicación efectiva, tanto dentro de la organización como con las autoridades y otras partes interesadas. La transparencia en la comunicación fue crucial para coordinar la respuesta y asegurar que se tomaran las medidas adecuadas.
- Aislamiento y contención: la compañía tomó medidas para aislar las partes afectadas de su red y evitar la propagación del ransomware. La contención del ataque ayudó a proteger otros sistemas y datos que no estaban comprometidos.
- Recuperación y restauración: una vez que el ataque fue contenido, la empresa trabajó en la recuperación y restauración de los sistemas afectados. Esto implicó la eliminación del *ransomware* y la restauración de datos a partir de copias de seguridad previas.

El ataque de WannaCry a esta empresa resalta la importancia de contar con una sólida gestión de incidentes en las organizaciones. La detección temprana, la respuesta rápida y la implementación de medidas de contención son fundamentales para minimizar el impacto de los ciberataques y proteger la continuidad del negocio y la seguridad de los datos. La gestión de incidentes también incluye la comunicación efectiva y la planificación del proceso de recuperación y restauración después del ataque.

Los estándares internacionales juegan un papel importante para establecer acciones efectivas y respuestas rápidas ante incidentes en las organizaciones. Entre los estándares y marcos de referencia a nivel global más destacados en gestión de incidentes están ISO/IEC 27035-2, ISO/IEC 27037, ISO/IEC 27039 y NIST 800-61.

ISO/IEC 27035-2:2023. Tecnología de la información – Gestión de incidentes de seguridad de la información – Parte 2: Directrices para planificar y preparar la respuesta a incidentes[23]

Este documento proporciona directrices para

planificar y preparar la respuesta ante incidentes y para aprender lecciones luego de dar respuesta a los mismos. Las directrices se basan en las fases de "planificación y preparación" y "aprendizaje de lecciones".

Los puntos principales dentro de la fase de "planificar y preparar" incluyen contar con:

- Una política de gestión de incidentes de seguridad de la información y compromiso de la alta dirección.
- Políticas de seguridad de la información, incluidas las relativas a la gestión de riesgos, actualizadas tanto a nivel organizativo como de sistemas, servicios y redes.
- Un plan de gestión de incidentes de seguridad de la información.
- Un Equipo de Gestión de Incidentes (IMT, por sus siglas en inglés).
- Relaciones y conexiones con organizaciones internas y externas.
- Apoyo técnico y de otro tipo (incluido el apoyo organizativo y operativo).
- Sesiones informativas y formación sobre la gestión de incidentes de seguridad de la información.

La fase de "aprendizaje de lecciones" se enfoca en la:

- Identificación de áreas susceptibles de mejora.
- Identificación y realización de las mejoras necesarias.
- Evaluación del Equipo de Respuesta a Incidentes (ERI).

ISO/IEC 27037:2012. Tecnología de la información – Técnicas de seguridad – Directrices para la identificación, recogida, adquisición y conservación de pruebas digitales[24]

ISO/IEC 27037:2012 brinda las directrices para actividades específicas en el manejo de evidencia digital, como son la identificación, recolección, adquisición y preservación de evidencia digital potencial que puede tener valor probatorio.

De igual forma, orienta con respecto a situaciones comunes encontradas a lo largo del proceso de manejo de evidencia digital, y ayuda a las organizaciones en sus procedimientos disciplinarios y en facilitar el intercambio de evidencia digital potencial entre jurisdicciones.

ISO/IEC 27039:2015. Tecnología de la información – Técnicas de seguridad – Selección, despliegue y operación de sistemas de detección y prevención de intrusiones (IDPS)[25]

ISO/IEC 27039:2015 proporciona los lineamientos para ayudar a las organizaciones a prepararse para desarrollar sus sistemas de detección y prevención de intrusiones (IDPS, por sus siglas en inglés). En particular, aborda la selección, despliegue y operación de IDPS. También proporciona información de fondo de la que se derivan estas directrices.

NMX-I-22301-NYCE-2021 | ISO 22301:2019. Tecnologías de la información – Seguridad y resiliencia – Sistemas de gestión de la continuidad del negocio – Requerimientos[26]

Establece los requisitos para implementar, mantener y mejorar continuamente un sistema de gestión para protegerse contra amenazas, reducir la probabilidad de su ocurrencia, y prepararse para responder y recuperarse de las interrupciones cuando se presenten incidentes.

Los elementos relevantes de este estándar son la gestión de riesgos, el análisis de impacto al negocio (BIA, por sus siglas en inglés), la identificación y selección de estrategias de continuidad, y la definición de tiempos: objetivo de tiempo de recuperación de evento disruptivo (RTO, por sus siglas en inglés); objetivo de punto de recuperación (RPO, por sus siglas en inglés), el cual determina la cantidad máxima aceptable de pérdida de datos (en minutos u horas) que la empresa se puede permitir; tiempo máximo de inactividad tolerable (MTD, por sus siglas en inglés), que define la cantidad total de tiempo que un proceso de negocio puede interrumpirse

sin causar consecuencias inaceptables. De igual manera destacan los planes de continuidad del negocio (BCP, por sus siglas en inglés), los planes de recuperación ante desastres (DRP, por sus siglas en inglés), las estructuras de advertencia, comunicación y respuesta, los programas de ejercicios (pruebas), y la evaluación de capacidades de continuidad.

ISO/IEC 22361:2022. Seguridad y resistencia – Gestión de crisis[27]

Este estándar ofrece orientación sobre la identificación y gestión de crisis en las empresas. Ayuda a las organizaciones a planificar, establecer, mantener, revisar y mejorar continuamente su capacidad estratégica de gestión ante crisis. Incluye, entre otros, recomendaciones para el desarrollo de la capacidad de gestión de crisis de una organización, el liderazgo ante crisis, la toma de decisiones a las que se enfrenta un equipo de crisis en acción y la comunicación de las mismas. Estas recomendaciones se dirigen tanto a la Junta Directiva, como a quienes son responsables de las operaciones.

ISO/IEC 27031:2011. Tecnología de la información – Técnicas de seguridad – Guía sobre preparación de tecnologías de la información y la comunicación para la continuidad del negocio[28]

Describe los conceptos y principios de la preparación de las tecnologías de la información y la comunicación (TIC) para la continuidad del negocio, y proporciona un marco de métodos y procesos para identificar y especificar todos los aspectos (como criterios de desempeño, diseño e implementación) para mejorar la preparación de las TIC de una organización y así garantizar la continuidad del negocio, incluyendo eventos e incidentes relacionados con la seguridad que podrían tener un impacto en la infraestructura y los sistemas de TIC. Incluye y amplía las prácticas de manejo y gestión de incidentes de seguridad de la información y planificación y los servicios de preparación de las TIC.

Marcos de referencia relevantes

NIST 800-61. Guía de gestión de incidentes de seguridad informática[29]

Esta guía fue desarrollada por el NIST como parte de sus responsabilidades estatutarias bajo la Ley de Gestión de Seguridad de la Información Federal (FISMA). Tiene como finalidad fortalecer las capacidades de respuesta de las organizaciones para hacer frente a incidentes de seguridad informática de manera efectiva, proporcionando pautas para analizar los datos relacionados con estos eventos y así determinar la respuesta apropiada. Las recomendaciones que contiene la guía pueden seguirse de manera independiente a plataformas de hardware particulares, sistemas operativos, protocolos o aplicaciones específicas.

5. Conclusión

// En el contexto actual, la ciberseguridad se ha vuelto un pilar esencial para la protección de empresas y organizaciones de todos los tamaños. La creciente sofisticación de las amenazas cibernéticas, la interconexión digital de los sistemas y la rápida evolución de la tecnología han creado un escenario en el que la seguridad de la información es una prioridad ineludible. En este sentido, los estándares internacionales de ciberseguridad desempeñan un papel de vital importancia al proporcionar un marco coherente y reconocido a nivel mundial.

© Polycube/Freepik

Estos estándares no son simplemente conjuntos de reglas abstractas; son una guía sólida basada en buenas prácticas y experiencias acumuladas a nivel global. Representan un esfuerzo conjunto de expertos en ciberseguridad, gobiernos, instituciones y organizaciones internacionales para definir los requisitos y prácticas recomendadas que garantizan la protección efectiva de la información. Su aplicación permite a las empresas y organizaciones de todas las industrias y sectores diseñar, desarrollar, implementar y mantener estrategias de protección cibernética efectivas.

La ciberseguridad es un campo en constante evolución. Las ciberamenazas no permanecen estáticas; evolucionan y se sofistican continuamente. En este escenario, los estándares internacionales ofrecen una ventaja crucial al adaptarse a los cambios en el panorama de amenazas y proporcionar orientación actualizada. Además, estos estándares proporcionan un marco que permite a las organizaciones cumplir con las regulaciones y requisitos legales, lo que es especialmente relevante en un entorno donde la privacidad de los datos y la protección de la información son cuestiones críticas.
Partiendo de este contexto, este documento, elaborado en el marco del Dialogo Mexicano-Alemán en Infraestructura de la Calidad, por un grupo de expertos de la industria y de organismos de estandarización y evaluación de la conformidad, proporciona un mapeo de los más relevantes estándares internacionales de ciberseguridad. Presentando las referencias internacionales para distintos elementos de una estrategia de ciberseguridad, como lo son la gestión de riesgos, herramientas de protección y gestión de incidentes, así como lineamientos de protección para aplicaciones específicas como las redes industriales, busca proporcionar orientación a empresas en México que buscan robustecer sus políticas de ciberseguridad.

En resumen, los estándares internacionales de ciberseguridad representan una brújula esencial para las organizaciones que buscan fortalecer su postura de seguridad cibernética. Ayudan a navegar un entorno cada vez más complejo, aseguran el cumplimiento de regulaciones y requisitos legales, y fomentan la colaboración global en la lucha contra las ciberamenazas. La ciberseguridad es un desafío constante, y la adopción de estándares internacionales es un paso esencial hacia la protección de la información en un mundo altamente interconectado.

6. Referencias

[1] Ver, por ejemplo, UNIDO (2006). The Role of Standards.

[2] DOF (2015). Declaratoria de vigencia de las normas mexicanas NMX-I-25021-NYCE-2015, NMX-I-27001-NYCE-2015 y NMX-I-27002-NYCE-2015.

[3] RiskOptics (2023). What is a Cybersecurity Framework?

[4] RiskOptics (2023). What is a Cybersecurity Framework?

[5] ISO (2021). ISO/IEC 27036-1:2021.

[6] ISO (2021). ISO/IEC 27036-1:2021.

[7] NYCE (2019). NMX-I-27005-NYCE-2019.

[8] ISO (2022). ISO/IEC 27005:2022.

[9] ISO (2018). ISO 31000:2018.

[10] ISO (2022). ISO 27557:2022.

[11] ISO (2019). ISO/IEC 31010:2019.

[12] NIST. Security Controls.

[13] NIST. Hardening.

[14] ISO (2022). ISO/IEC 27002:2022.

[15] ISO (2019). ISO/IEC 27008:2019.

[16] ISO (2021). ISO/IEC 27022:2021.

[17] ISO (2015). ISO/IEC 27033:2015.

[18] ISO (2016). ISO/IEC 27004:2016.

[19] ISO (2015). ISO/IEC 27017:2015.

[20] ISO (2019). ISO/IEC 27018:2019.

[21] ISA/IEC (2009). ISA/IEC 62443-2-1-2009.

[22] ISA/IEC (2009). ISA/IEC 62443-3-1:2009.

[23] ISO (2023). ISO/IEC 27035:2023.

[24] ISO (2012). ISO/IEC 27037:2012.

[25] ISO (2015). ISO/IEC 27039:2015.

[26] NYCE (2021). NMX-I-22301-NYCE-2021.

[27] ISO/IEC (2022). ISO/IEC 22361:2022.

[28] ISO/IEC (2011). ISO/IEC 27031:2011.

[29] NIST (2012). NIST 800-61 Computer Security Incident Handling Guide.

ANEXO 1. Marco legal: leyes en México relacionadas a la ciberseguridad

Tema	Ley y artículos relevantes
Privacidad de los usuarios y la seguridad de la red	Ley Federal de Telecomunicaciones y Radiodifusión, Art. 145.III
Datos personales	• Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Art. 19 y 21 • Ley General Protección de Datos Personales en Posesión de Sujetos Obligados, Art. 2.XIV, 31, 42, 59, 64 i.d), 67 y 82
Información confidencial APF	Ley General de Transparencia y Acceso a la Información Pública, Art. 116-120
Información privilegiada	Ley del Mercado de Valores, Art. 362, 363, 364, 380, 381 y 392
Secreto bancario y fiduciario	• Ley de Instituciones de Crédito, Art. 46 bis y 142 • Circular Única Bancaria, Art. 326 bis 10
Secreto industrial	Ley de Protección a la Propiedad Industrial, Art. 163-169
Secreto profesional	Ley Reglamentaria del Artículo 5º Constitucional
Secreto comunicación reservada	Código Penal Federal, Art. 210-211 bis
Secretos de fabricación, técnicos y comerciales	Ley Federal del Trabajo, Art. 46.IX, 134.XIII
Secreto médico profesional	NOM-004-SSA3-2012. Del Expediente Clínico Electrónico, Art. 5.4, 5.5.1, 5.7
Secreto societario	Ley General de Sociedades Mercantiles, Art. 157
Seguridad nacional	Ley de Seguridad Nacional, Art. 6.V, 10, 53, 61, 63
Secreto de los datos del consumidor	• Ley Federal de Protección al Consumidor, Art. 76 bis I y II • NMX-COE-001-SCFI-2018. Comercio Electrónico, Art. 8 y 10.4.1

ANEXO 2. Estándares internacionales de ciberseguridad

Estándares nacionales basados en estándares internacionales
NMX-I-27001-NYCE-2015 | ISO/IEC 27001:2015. Tecnologías de la información –Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requisitos
NMX-I-27002-NYCE-2015 | ISO/IEC 27002:2022. Tecnologías de la información – Seguridad de la información, ciberseguridad y protección de la privacidad – Controles de seguridad de la información
NMX-I-27005-NYCE-2019 | ISO/IEC 27005:2018. Tecnologías de la información – Técnicas de seguridad – Gestión de riesgos en seguridad de la información
NMX-I-27032-NYCE-2018 | ISO/IEC 27032. Tecnologías de la información – Técnicas de seguridad – Lineamientos para la ciberseguridad
NMX-I-22301-NYCE-2021 | ISO 22301:2019. Tecnologías de la información – Seguridad y resiliencia – Sistemas de gestión de la continuidad del negocio – Requerimientos

Estándares básicos de vocabulario y definiciones
ISO/IEC 27000:2018. Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información – Visión general y vocabulario
ISO/IEC 27033-1:2015. Tecnología de la información – Técnicas de seguridad – Seguridad de red – Parte 1: Visión general y conceptos
ISO/IEC 27034-1:2011. Tecnología de la información – Técnicas de seguridad – Seguridad de las aplicaciones – Parte 1: Visión general y conceptos
ISO/IEC 27036-1:2021. Ciberseguridad – Relaciones con los proveedores – Parte 1: Visión general y conceptos

Estándares de gestión de riesgos
ISO/IEC 27005:2022. Tecnologías de la información – Técnicas de seguridad – Gestión de riesgos en seguridad de la información
ISO/IEC 31000:2018. Gestión de riesgos – Lineamientos
ISO/IEC 27557:2022. Seguridad de la información, ciberseguridad y protección de la privacidad – Aplicación de la norma ISO 31000:2018 para la gestión del riesgo de privacidad organizacional
ISO/IEC 31010:2019. Gestión de riesgos – Técnicas de evaluación de riesgos

Estándares de controles e implementación
ISO/IEC 27002:2022. Seguridad de la información, ciberseguridad y protección de la privacidad – Controles de seguridad de la información
ISO/IEC 27008:2019. Informática – Técnicas de seguridad – Directrices para la evaluación de los controles de seguridad de la información
ISO/IEC TS 27022:2021. Tecnología de la información – Orientación sobre los procesos del sistema de gestión de la seguridad de la información
ISO/IEC 27004:2016. Tecnología de la información – Técnicas de seguridad – Gestión de la seguridad de la información – Seguimiento, medición, análisis y evaluación
ISO/IEC TS 27008:2019. Information technology – Security techniques – Guidelines for the assessment of information security controls
ISO/IEC 15408:2022. Seguridad de la información, ciberseguridad y protección de la privacidad – Criterios de evaluación de la seguridad informática

Estándares para aplicaciones en la nube
ISO/IEC 27017:2015. Tecnología de la información – Técnicas de seguridad – Código de buenas prácticas para los controles de seguridad de la información basados en la norma ISO/IEC 27002 para servicios en la nube
ISO/IEC 27018:2019. Tecnología de la información – Técnicas de seguridad – Código de prácticas para la protección de la información de identificación personal (IIP) en nubes públicas que actúan como procesadores de IIP
Cloud Security Alliance – Cloud Controls Matrix https://cloudsecurityalliance.org/research/cloud-controls-matrix/

Estándares para redes industriales
ISA/IEC 62443-2-1-2009. Seguridad para sistemas de control y automatización industrial – Parte 2-1: Establecimiento de un programa de seguridad para sistemas de automatización y control industrial
ISA/IEC 62443-2-2. Seguridad para sistemas de control y automatización industrial – Parte 2-2: Niveles de protección de IACS
ISA/IEC 62443-2-5:2020. Seguridad para sistemas de control y automatización industrial – Parte 2-5: Guías de implementación para los propietarios de activos del SGC
ISA/IEC 62443-3-1:2009. Redes de comunicación industriales – Seguridad de redes y sistemas – Parte 3-1: Tecnologías de seguridad para sistemas de control y automatización industrial
ISA/IEC 62443-3-2:2020. Seguridad para los sistemas de control y automatización industrial – Parte 3-2: Evaluación de riesgos de seguridad para el diseño de sistemas
ISA/IEC 62443-4-1:2018 | NMX-I-62443-4-1-NYCE-2021. Electrónica – Seguridad para los sistemas de control y automatización industrial – Parte 4-1: Requisitos del ciclo de vida del desarrollo seguro del producto

Estándares de gestión de incidentes
ISO/IEC 27031:2011. Tecnologías de la información – Técnicas de seguridad – Guía sobre preparación de tecnologías de la información y la comunicación para la continuidad del negocio
ISO/IEC 27035-2:2023. Tecnología de la información – Gestión de incidentes de seguridad de la información – Parte 2: Directrices para planificar y preparar la respuesta a incidentes
ISO/IEC 27037:2012. Tecnología de la información – Técnicas de seguridad – Directrices para la identificación, recogida, adquisición y conservación de pruebas digitales
ISO/IEC 27039:2015. Tecnología de la información – Técnicas de seguridad – Selección, despliegue y operación de sistemas de detección y prevención de intrusiones (IDPS)
NMX-I-22301-NYCE-2021 | ISO 22301:2019. Tecnologías de la información – Seguridad y resiliencia – Sistemas de gestión de la continuidad del negocio – Requerimientos
ISO/IEC 22361:2022. Seguridad y resistencia – Gestión de crisis

ANEXO 3. Estándares de ciberseguridad para sectores y actividades específicos

Estándar	Descripción | Beneficios e importancia
ISO/IEC 27009:2020 Information Security, Cybersecurity and Privacy Protection – Sector-specific application of ISO/IEC 27001 – Requirements	Este documento señala los requisitos para crear estándares específicos del sector que amplían ISO/IEC 27001 y complementan o modifican ISO/IEC 27002 para respaldar un sector específico (dominio, área de aplicación o mercado).

Sector	Estándar
Telecomunicaciones	• ISO/IEC 27011:2016/COR 1:2018 • Information technology – Security techniques – Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations – Technical Corrigendum 1
Teletrabajo	NMX-I-309-NYCE-2019. Tecnologías de la información – Seguridad de la información en el teletrabajo
Servicios en la nube	• ISO/IEC 27017:2015. Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services • Cloud Security – European Union Agency for Cybersecurity (ENISA)
Energía	ISO/IEC 27019:2017. Information technology – Security techniques – Information security controls for the energy utility industry
Redes	ISO/IEC 27033. Information technology – Security techniques – Network security (Family)
Sistemas y aplicaciones	ISO/IEC 27034-2:2015. Information technology – Security techniques – Application security
Salud	ISO/IEC 27999:2016. Health informatics – Information security management in health using ISO/IEC 27002
Transporte	ISO/SAE 21434:2021. Road vehicles – Cybersecurity engineering

ANEXO 4. Marcos internacionales de referencia relacionados a la ciberseguridad

Marco
NIST Cybersecurity Framework, versión 1.0
NIST SP 800-53B. Líneas base de control para sistemas de información y organizaciones
NIST Risk Management Framework (RMF) – Marco de Gestión de Riesgos
COBIT 2019: Con área de enfoque en seguridad de la información
NIST 800-61. Guía de gestión de incidentes de seguridad informática