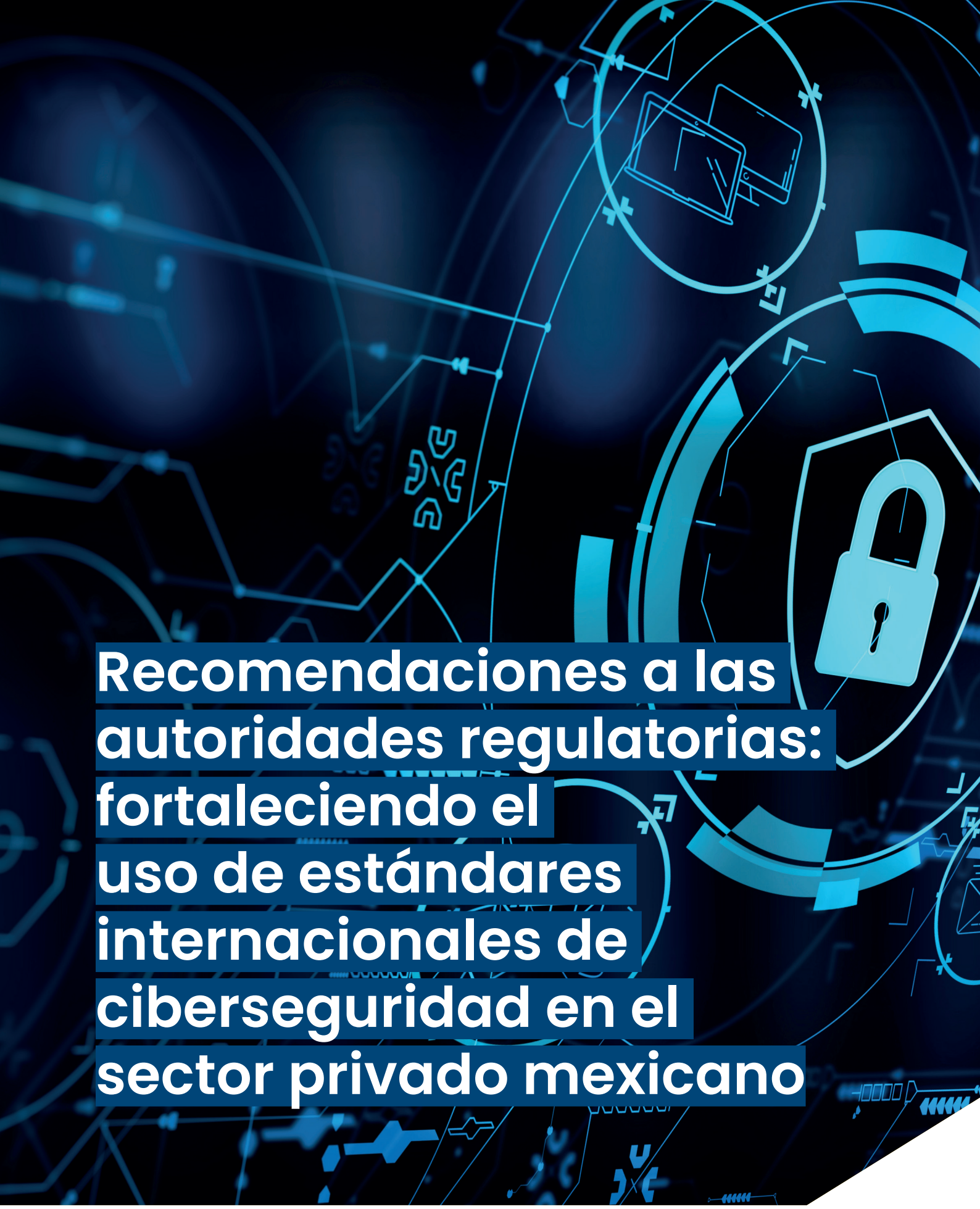


Recomendaciones a las autoridades regulatorias: fortaleciendo el uso de estándares internacionales de ciberseguridad en el sector privado mexicano

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: user12683362/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

Federal Ministry
for Economic Affairs
and Climate Action

giz Deutsche Gesellschaft
für Internationale
Zusammenarbeit (GIZ) GmbH

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 es el tercero de cuatro volúmenes sobre la importancia de la ciberseguridad en las empresas y del papel que tiene el uso de estándares armonizados internacionalmente para la ciberseguridad y la seguridad de la información a lo largo de las cadenas de valor. 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.....6

2. Marco legal de ciberseguridad en México.....8

3. Normas Oficiales Mexicanas y estándares de ciberseguridad en México.....9

4. Recomendaciones para fortalecer la ciberseguridad en el sector privado.....10

4.1 Realizar un mapeo del estado de madurez en lo relativo a ciberseguridad en las empresas.....11

4.2 Fomentar la cooperación regulatoria internacional en materia de ciberseguridad.....13

4.3 Fortalecer las capacidades de ciberseguridad en el personal y las políticas y procesos de gestión de ciberseguridad de las empresas.....14

4.4 Promover la certificación de empresas en ISO 27001 e IEC 63443.....17

4.5 Adoptar otros estándares internacionales complementarios a ISO 27001 e IEC 62443.....19

5. Conclusión.....20

6. Referencias.....21

1. Introducción

// De acuerdo con datos de la Guardia Nacional, de enero de 2019 a abril de 2022, en México se presentaron más de 223,600 incidentes de seguridad cibernética cometidos contra empresas, bancos, universidades e instituciones públicas. Los principales vectores de ataque fueron la infección de equipos con códigos maliciosos, la creación de sitios falsos y el uso de ransomware. Esta tendencia va en aumento: tan sólo en el primer semestre de 2022, México recibió 80,000 millones de intentos de ciberataques, lo que representa más de la mitad de los ataques contabilizados en 2021 y convierte al país en el más atacado a nivel Latinoamérica (Forbes, 2022).

© KanawatTH/Freepik

El sector privado ha sido particularmente afectado. Según el estudio de Deloitte "Consideraciones de Ciberseguridad en Medio de una Pandemia Global", el 62% de las empresas en México han sufrido ciberataques desde el inicio de la pandemia y al menos el 76% de las empresas han sufrido uno o dos ataques significativos al año (Deloitte, 2020). El robo y secuestro de información, la paralización de sistemas operativos y la publicación de información confidencial son sólo algunos de los incidentes de ciberseguridad que pueden afectar a las empresas. Estos pueden impactar en daños como pérdidas económicas, afectación de relaciones empresariales, y hasta poner en riesgo el mismo negocio de la empresa. En este sentido, el 54% de los ataques resultan en daños financieros, incluidos pérdidas de ingresos, clientes, oportunidades, y otro tipo de costos monetarios (Olivera, 2023). Ante este panorama no resulta sorprendente que los ataques cibernéticos sean aquellas amenazas que las empresas en México consideran más probables de materializarse (Hernández, 2022).

Dentro del sector privado, las empresas más vulnerables han sido las PyMEs, que a menudo no cuentan con sistemas de protección suficientes y, por ende, se han convertido en un blanco popular entre los ciberdelincuentes (Forbes, 2020). De este modo, en 2020, el número de ataques de ransomware en Latinoamérica hacia las PyMEs aumentaron un 424%. El costo promedio de un pago de rescate para una PyME en México ha sido de 2 millones de pesos, según datos de la última encuesta de la Asociación de Internet MX a inicios de este año (Zamarrón, 2023).

En México, las PyMEs son un motor clave de un desarrollo económico incluyente, ya que generan el 72% del empleo formal en el país y son responsables de la generación del 52% del PIB. Esto convierte el robustecimiento de la ciberseguridad en el sector en una tarea estratégica para impulsar la economía del país (Senado de la República, 2020).

Los estándares internacionales juegan un papel fundamental en el robustecimiento de las condiciones de ciberseguridad en el sector privado: reúnen lineamientos para el desarrollo de estrategias de ciberseguridad considerando factores técnicos, de personal y de organización, además de herramientas para mitigar riesgos específicos de ciberseguridad. Son desarrollados a partir del conocimiento de expertos y expertas de diversos países y revisados de manera regular, por lo que constituyen herramientas

de vanguardia en la protección contra ciberataques. Más aún, dado su reconocimiento internacional, la certificación en estándares de ciberseguridad puede facilitar la integración de PyMEs a cadenas globales de valor y fortalecer su reputación en el mercado, en particular en sectores vulnerables a ciberataques. Estas características convierten a los estándares internacionales de ciberseguridad en una herramienta de protección y también de desarrollo económico.

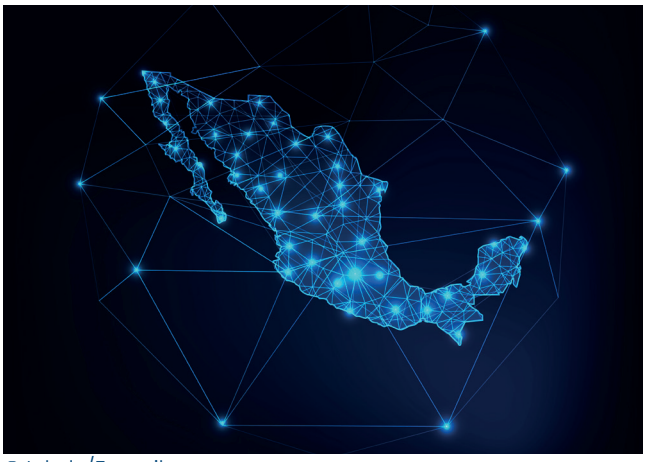
El presente documento pretende reunir recomendaciones para las autoridades responsables en materia de ciberseguridad en México sobre los estándares internacionales más importantes y sobre el desarrollo de capacidades necesarias para su implementación en el sector privado, en especial en las PyMEs.

A partir del marco regulatorio actual y recientes iniciativas, se presentan recomendaciones estratégicas de estandarización, fomento de capacidades en las empresas, formación de la fuerza laboral de ciberseguridad y cooperación internacional. Estas fueron elaboradas por un grupo de especialistas de empresas y asociaciones empresariales, organismos de estandarización y evaluación de la conformidad y autoridades en telecomunicaciones, desde la práctica y el conocimiento de la situación de ciberseguridad en el país.

2. Marco legal de ciberseguridad en México

// El panorama de crecientes ciberamenazas pone de manifiesto la necesidad de contar con un marco regulatorio que permita abordar esta situación desde la perspectiva legal. Si bien es cierto que en el Código Penal Federal Art. 211 y Art. 140 bis se tipifican y sancionan algunas de las conductas que constituyen ciberdelitos y que hoy en día existen cinco iniciativas de ley de ciberseguridad en el Senado de la República –pendientes en la Comisión de Justicia para su análisis y dictamen–, aún no se cuenta con ninguna ley de ciberseguridad. En cuanto a la protección de datos personales, en México se cuenta con la Ley de Protección de Datos Personales en Posesión de los Particulares, que busca "la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas" (Congreso de la Unión, 2010).

Durante las LXIV y LXV Legislaturas se registraron varias iniciativas sobre ciberseguridad en el Congreso de la Unión, de las cuales nueve corresponden a la Cámara de Diputados y siete al Senado de la República. A manera de resumen, dos iniciativas proponen reformar el artículo 73 constitucional, otra más el artículo 21 constitucional; seis, modificar varios ordenamientos (Código Penal Federal, Ley General del Sistema Nacional de Seguridad Pública, Ley de Seguridad Nacional, Ley Federal de Austeridad Republicana, Ley de la Fiscalía General de la República); otras dos, a elaborar una nueva ley; cuatro plantearon reformar y expedir nuevos ordenamientos (como una Ley General de Ciberseguridad), y dos más, a conmemorar un día y un mes nacional de la ciberseguridad.



© Inkoly/Freepik

Las iniciativas de ley prevén crear un marco legal que permita tipificar y sancionar ciberataques, crear un Registro Nacional de Incidentes de Ciberseguridad y una Agencia Nacional de Ciberseguridad similar a los modelos seguidos en la Unión Europea (UE), EE. UU. y Brasil.

3. Normas Oficiales Mexicanas y estándares de ciberseguridad en México

// En la actualidad, en México no existen Normas Oficiales Mexicanas (NOM) que especifiquen lineamientos obligatorios de ciberseguridad. Sin embargo, existen varios estándares (antes Normas Mexicanas o NMX) que plantean estrategias y herramientas para fortalecer la ciberseguridad de las empresas. En particular, en México ya se adoptaron los estándares internacionales ISO/IEC 27001 e IEC 62443 como NMX-I-27001-NYCE-2015 y NMX-I-62443-4-1-NYCE-2021, correspondientemente. Dada su naturaleza como estándares, a la fecha, su implementación y certificación es voluntaria, ya que no se encuentran referenciados en una NOM. Al tratarse de estándares internacionales elaborados por expertos y expertas de múltiples países y regiones, reúnen las mejores prácticas internacionales de vanguardia y crean un marco de referencia común a nivel internacional, lo que facilita el reconocimiento transfronterizo de empresas certificadas y reduce barreras técnicas para el comercio.

El estándar ISO/IEC 27001 regula los sistemas de gestión de la seguridad de la información (SGSI): define los requisitos mínimos que debe cumplir un SGSI y proporciona a las empresas orientación para desarrollar, implementar y mejorar de manera continua un sistema de gestión de la seguridad de la información. Se trata de un estándar genérico, aplicable a empresas de diversos tamaños y sectores. En resumen, la conformidad con ISO/IEC 27001 significa que una organización o empresa ha implantado un sistema para gestionar los riesgos relacionados con la seguridad de los datos que posee o maneja, y que este sistema respeta todas las buenas prácticas y principios consagrados en este estándar internacional (ISO, 2022a).

Por su parte, IEC 62443 es un estándar más específico que define los requisitos y procesos para implantar y mantener sistemas de automatización y control industrial (IACS) electrónicamente seguros. Establece el punto central de referencia internacional sobre 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 (IEC, 2021).

Sin embargo, aunque estos dos estándares internacionales ya se adoptaron en México, los datos muestran que pocas empresas han buscado la certificación. De acuerdo con el reporte de ISO Survey 2022, en México sólo hay 279 empresas certificadas en ISO 27001, lo que impide que en la situación actual estos estándares puedan contribuir de manera significativa a una mejora de las condiciones de ciberseguridad en el país (ISO, 2022b).

4. Recomendaciones para fortalecer la ciberseguridad en el sector privado

// Ante este panorama, se plantea un conjunto estratégico de acciones para fortalecer la implementación de estándares internacionales de ciberseguridad en las empresas, a fin de impulsar el desarrollo de capacidades a nivel individual y organizacional y crear condiciones marco correspondientes. Dichas acciones estratégicas se nutren de dos campos de acción transversales: la mejoría de la información disponible sobre las condiciones de ciberseguridad en las empresas mexicanas y el fortalecimiento de los mecanismos de cooperación regulatoria internacional con ejemplos de buenas prácticas y experiencias de otros países como guía en el diseño.

En este sentido, se contemplan cinco recomendaciones estratégicas: 1) realizar un mapeo del estado de madurez en lo relativo a ciberseguridad en las empresas que operan en México; 2) fomentar la cooperación regulatoria internacional en materia de ciberseguridad; 3) fortalecer las capacidades de ciberseguridad en a) el personal y b) las políticas y procesos de gestión de ciberseguridad de las empresas; 4) fomentar la certificación de empresas en ISO 27001 en sectores críticos, y 5) adoptar otros estándares internacionales complementarios a ISO 27001 e IEC 62443 para ponerlos a disposición de empresas mexicanas. La figura 1 muestra cómo estas acciones actúan en conjunto a nivel individual, organizacional y de marco regulatorio para robustecer las condiciones de ciberseguridad en el sector privado mediante la promoción de la implementación de estándares internacionales.

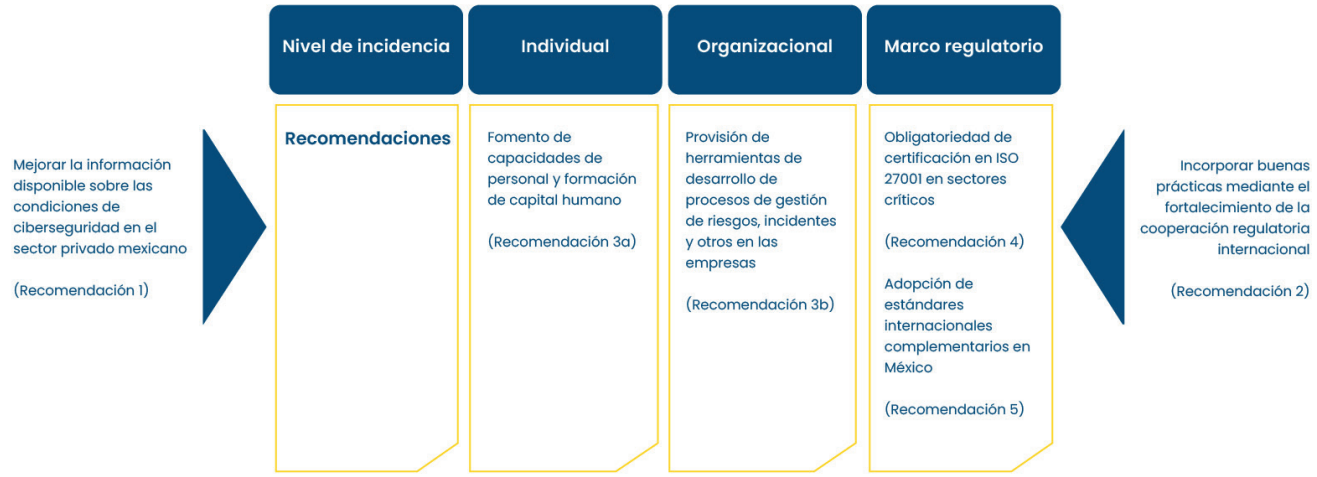


Gráfico 1. Elementos estratégicos para fortalecer la ciberseguridad en el sector privado mexicano mediante la implementación de estándares y la creación de capacidades para ello. Elaboración propia.

Es importante resaltar varios puntos respecto a estas recomendaciones. Primero, se trata de recomendaciones interdependientes. Por ejemplo, el fortalecimiento de procesos de gestión de ciberseguridad en las empresas depende de contar con acceso a personal capacitado. Por otro lado, la obligatoriedad de certificación en actividades y sectores críticos ayuda a incentivar la capacitación.

Otro punto a destacar es que la información a detalle, por sectores, tamaños de empresa y territorios que se busca generar a partir de la recomendación 1) es un insumo fundamental en diseñar acciones diferenciadas dentro de los ejes individual, organizacional y condiciones marco. El otro ingrediente principal en el diseño es la guía de buenas prácticas universales mediante el fomento de la cooperación regulatoria internacional.

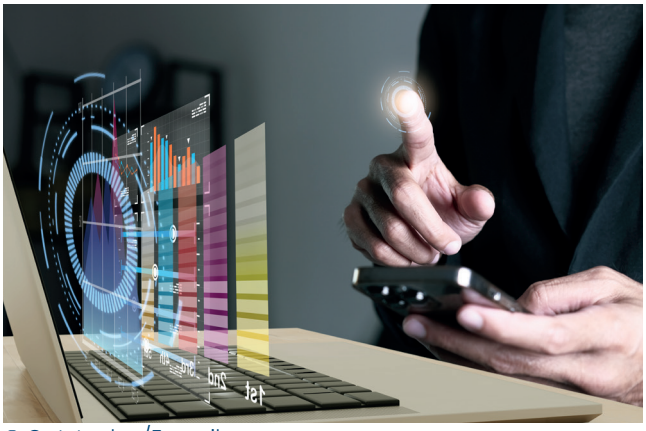
A continuación se profundizará en cada una de estas recomendaciones.

4.1 Realizar un mapeo del estado de madurez en lo relativo a ciberseguridad en las empresas

Antecedentes

Antes de desarrollar una estrategia de ciberseguridad en el sector privado, es necesario reconocer la gran diferencia en cuanto a tamaño, actividades, capital humano y madurez digital de las empresas. Cada empresa enfrenta diferentes peligros, e incluso en algunas de ellas lo que puede estar en riesgo son infraestructuras críticas o bien cadenas de valor completas que podrían, en caso de verse perjudicadas, afectar la economía nacional. Por otra parte, existen distintas capacidades y recursos para enfrentar las amenazas en materia de ciberseguridad, así que es claro que no se pueden dirigir las mismas medidas o establecer los mismos requisitos para todas las empresas.

Ante este panorama, resulta importante mejorar el conocimiento de los niveles de madurez en ciberseguridad en empresas de



© Oatstocker/Freepik

distintos sectores, actividades y tamaños, a fin de poder desarrollar programas a la medida que impulsen a las empresas a capacitarse y generar estrategias orientadas al cumplimiento de estándares internacionales. Esta recomendación va encaminada a que se tenga un mapeo estandarizado del nivel de madurez de las empresas por sector, por actividad económica, y región; lo importante es reconocer el punto de madurez que se tiene y a partir de ahí, emprender esfuerzos coordinados de desarrollo en este tema.

Propuesta

La implementación de medidas o tecnología de ciberseguridad en una empresa está, por lo general, alineada a un plan o estrategia. Dos de los elementos más importantes y necesarios que deberán formar parte de ese plan es una identificación de riesgos y un diagnóstico de madurez. El primero permitirá tener una radiografía de la organización y de sus procesos en donde se identifique cuáles de ellos son los más críticos para el negocio, cuáles son más susceptibles a ataques, cuáles son estratégicos en términos de ciberseguridad, etc. El segundo, el diagnóstico, le servirá a la organización para identificar el nivel de madurez actual de toda la organización con respecto a los controles implementados, las políticas existentes, el nivel de conocimiento de los empleados, la conciencia colectiva sobre los posibles riesgos, la tecnología utilizada y demás factores organizacionales y tecnológicos.

A partir de estos dos elementos, la organización podrá tener conciencia de su situación particular

y, con ello, definir un plan de implementación u hoja de ruta con medidas de ciberseguridad tanto tecnológicas como organizacionales basándose en la prioridad revelada por el análisis de riesgos y por el análisis de madurez (Cybersecurity Maturity Assessment).

Se propone impulsar la implementación del análisis de madurez en ciberseguridad de manera similar a como ya se realizan los análisis de madurez digital, a fin de permitir a las empresas conocer el nivel de avance que tienen, desde el nivel de capacidades de los empleados y empleadas, hasta la parte tecnológica y de procesos. En este tenor, una posibilidad es la creación de recursos en temas de ciberseguridad, gratuitos y de fácil acceso, como lo es la plataforma Digitalízate, la cual es una guía para simplificar la digitalización de las PyMEs y fue puesta a disposición del público general por el Centro México Digital.

Tal como se mencionó arriba, además de ser una entrada para la creación de una estrategia de ciberseguridad para las empresas, la información de los niveles de madurez también es útil para ser analizada en un nivel superior, ya sea por región, por tipo de empresa, sector económico, tipo de infraestructura, etc. De esta manera, las organizaciones como cámaras de comercio, asociaciones o incluso alguna dependencia de Gobierno o agencia puede acumular esa información y mapear el nivel de madurez de las empresas de acuerdo con alguno de los criterios mencionados. Toda esta información proveniente de empresas públicas, privadas o mixtas podría ser estudiada desde una visión macro y sobre ello diseñar programas y políticas específicas para fortalecer diversos aspectos de la ciberseguridad con un enfoque a nivel nacional.

Ahora bien, es importante hacer notar que en el mercado existe una oferta muy amplia de evaluaciones o diagnósticos de madurez de este tipo. Sin embargo, muchas de esas herramientas tienen un sesgo hacia cierta tecnología, de manera que el resultado de ese diagnóstico, así como las medidas de mejora sugeridas, suelen encaminarse a la adopción de ciertos productos o cierta marca específica. Por ello, lo más conveniente es que el diseño de ese diagnóstico de madurez, así como las recomendaciones resultantes se basen enteramente en estándares internacionales probados y aceptados.

En lo que incumbe al ámbito industrial, uno de los estándares con mayor aceptación debido a su gran alcance y robustez es IEC 62443. Un diagnóstico de madurez de ciberseguridad basado en este estándar tendría diversos enfoques tal como lo plantean las diferentes partes que lo integran, de manera que se evaluaría no sólo el aspecto tecnológico sino el organizacional y el operativo. Esto, sin duda, tiene muchas ventajas, pues no sólo toma las mejores prácticas de la industria a nivel internacional –lo cual tendría beneficios para las empresas–, sino que buscaría homologar la interacción a lo largo de las cadenas de valor y la infraestructura crítica.

En México existen dependencias como el Centro de Respuesta a Incidentes Cibernéticos de la Dirección General Científica de la Guardia Nacional (CERT-Mx) y mecanismos interinstitucionales como la Comisión Intersecretarial de Tecnologías de la Información y Comunicación, y de la Seguridad de la Información, cuyo objetivo es establecer un mecanismo de coordinación y conducción colegiada de acciones para la implementación de las políticas federales en estas materias. Dichos mecanismos interinstitucionales, con el apoyo de aliados tecnológicos, podrían poner a la disposición de las PyMEs una herramienta open source para analizar su nivel de madurez.

En la Unión Europea, por ejemplo, existe el Análisis de Madurez de Ciberseguridad para Pequeñas y Medianas Empresas, impulsado por la Agencia de la Unión Europea para la Ciberseguridad (ENISA). Este análisis incluye la esfera humana (analizar si los empleados están preparados para enfrentar ciberamenazas); la tecnología (para que la empresa entienda su tecnología y cómo implementar mejores prácticas de ciberseguridad), y los procesos (para asegurar que la organización tiene los procesos adecuados para lidiar con los riesgos cibernéticos.
Por otro lado, en EE. UU., existe el Modelo de

Madurez de las Capacidades de Ciberseguridad (C2M2) de la Oficina de Ciberseguridad, Seguridad Energética y Respuesta a Emergencias, una herramienta gratuita para ayudar a las organizaciones a evaluar sus capacidades de ciberseguridad y optimizar las inversiones respectivas. Utiliza un conjunto de prácticas de ciberseguridad validadas por la industria y centradas en activos y entornos tanto de tecnología de la información (TI), como de tecnología de operaciones (TO). Cualquier empresa, independientemente de su tamaño o sector, puede utilizar el modelo para evaluar, priorizar y mejorar sus capacidades de ciberseguridad.

4.2 Fomentar la cooperación regulatoria internacional en materia de ciberseguridad

Antecedentes

Mientras que el mapeo de madurez puede ayudar a mejorar la disponibilidad de la información requerida a fin de diseñar las acciones recomendadas para el fortalecimiento de la ciberseguridad, la cooperación regulatoria internacional sirve como un segundo elemento transversal para robustecer el desarrollo de estrategias con buenas prácticas internacionales. Mediante un conocimiento detallado del contexto, tal como se busca generar a partir de la recomendación anterior, estas estrategias se pueden adaptar y aterrizar a los distintos contextos mexicanos.

La Cooperación Regulatoria Internacional (CRI) se origina en la Recomendación del Consejo de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) sobre Política y Gobernanza Regulatoria de 2012, y tiene como objetivo promover la interoperabilidad de los marcos legales y regulatorios. La CRI es especialmente importante en un mundo cada vez más interconectado, donde las empresas operan a nivel internacional, y los problemas y riesgos trascienden las fronteras nacionales. La CRI permite a los países trabajar juntos para garantizar la eficiencia y la efectividad de las regulaciones, evitar barreras técnicas al comercio y promover

© Freepik

la confianza y la cooperación entre los actores internacionales.

En asuntos de ciberseguridad, la CRI promovería la colaboración, el intercambio de información y la armonización de estándares, lo que resultaría en una mejor implementación de medidas de seguridad cibernética en empresas de cualquier tamaño –incluidas las PyMEs–, a nivel mundial. Esto ayudaría a proteger los sistemas y datos de las organizaciones, así como a minimizar los riesgos y las amenazas en el entorno digital.

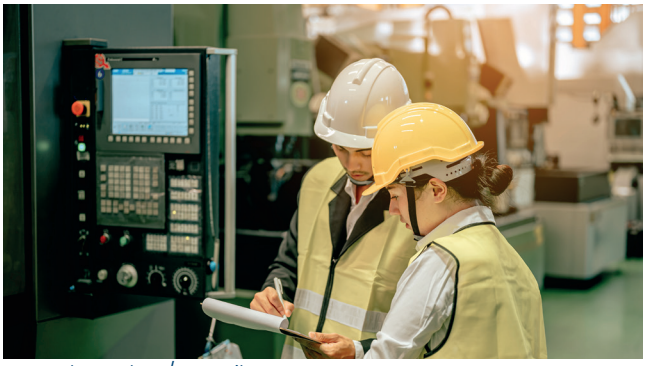
Propuesta

Se recomienda fomentar la CRI en el ámbito de la ciberseguridad. Esto puede desempeñar un papel crucial en la mejora de la implementación de estándares internacionales de ciberseguridad para las PyMEs de varias maneras:

1. Intercambio de información y mejores prácticas: la CRI facilita el intercambio de información y mejores prácticas en materia de ciberseguridad entre países y organizaciones internacionales. El intercambio de información entre agencias públicas de diversos países y organismos del sector privado es un mecanismo importante para comprender mejor un entorno de ciberamenazas que se encuentra en constante cambio, identificar vulnerabilidades críticas compartidas y desarrollar soluciones en conjunto. En este

contexto, la Agencia de la Unión Europea de Ciberseguridad (ENISA) elaboró una guía de cómo los países pueden instalar mecanismos de Intercambios de Información sobre Seguridad de las Redes (NSIEs, por sus siglas en inglés) que involucren también organismos del sector privado, lo cual también permite a las PyMEs acceder a conocimientos y experiencias de otros países y aprender de las mejores prácticas implementadas en diferentes contextos.

2. Armonización de regulaciones: la CRI busca la armonización de regulaciones en ciberseguridad. La armonización de regulaciones basadas en estándares internacionales facilita la adopción de medidas de ciberseguridad más efectivas y actualizadas, además de que reduce la complejidad y los costos asociados con el cumplimiento de diferentes regulaciones nacionales para empresas. En particular, para las PyMEs, el tener que cumplir con diferentes regulaciones técnicas y estándares para poder acceder a otros mercados o poder ganar como cliente a una empresa internacional, implica un costo adicional significativo que puede excluirlas de estas oportunidades económicas.
3. Capacitación, provisión de herramientas y concienciación: : la CRI puede proporcionar capacitación y concienciación sobre ciberseguridad a las PyMEs. Esto incluye la difusión de información sobre las amenazas y los riesgos de ciberseguridad, así como la promoción de buenas prácticas y medidas de protección. Por ejemplo, entre siete países de la Unión Europea se formó SMESEC, un proyecto propuesto por un grupo internacional de expertos y expertas como respuesta a los retos de ciberseguridad de las PyMEs con una formación limitada en ciberseguridad y un presupuesto restringido. En SMESEC se combinan experiencias y conocimientos de varios contextos nacionales para desarrollar soluciones de ciberseguridad de alta calidad atractivas para PyMEs con un presupuesto restringido, además de que se proporcionan capacitaciones para PyME y todo tipo de empleados.


© Nutthaseth-v/Freepik

4.3 Fortalecer las capacidades de ciberseguridad en el personal y las políticas y procesos de gestión de ciberseguridad de las empresas

Antecedentes

Existe una brecha creciente entre las amenazas de ciberseguridad –que, como ya se ha visto, van en aumento a grandes velocidades–, y las capacidades que existen en el sector privado, en particular entre las PyMEs, para enfrentarlas. Según el Informe de Brecha de Habilidades en Ciberseguridad de 2022, elaborado por Fortinet, un 86% de las PyMEs mexicanas no está preparada para amenazas y ocho de cada diez no cuenta con las herramientas necesarias de protección.

A esta falta de capacidades a nivel empresa se suma una escasez de talento en materia de ciberseguridad, no sólo en México sino a nivel mundial. De acuerdo con datos de Microsoft, la demanda de habilidades de ciberseguridad ha aumentado un 29% entre 2021 y 2022 en México. Conforme a la información de la Organización Internacional de Normalización (ISO), en la actualidad, en el país existe un déficit cercano a 400,000 expertos en ciberseguridad para poder cubrir la demanda creciente. Esto ha llevado a un aumento significativo de los salarios de los expertos y las expertas en ciberseguridad, sin que esto pueda incrementar la oferta a mediano plazo, lo cual reduce el acceso de las PyMEs a este recurso humano (OEA, 2023).

Ante este escenario, se plantea la necesidad de combinar una estrategia con elementos a largo plazo para incrementar la oferta de fuerza laboral en ciberseguridad, y medidas que a corto y mediano plazo puedan mejorar la capacidad organizacional de las PyMEs y les brinden guías para implementar políticas y procesos de ciberseguridad que les permitan hacer frente a las amenazas pese a no contar con un especialista propio.

Como resultado de esta doble necesidad, las propuestas se dividen en: a) recomendaciones para expandir el capital humano en ciberseguridad (mediano-largo plazo), y b) recomendaciones para facilitar la adopción de políticas y procesos de gestión de la ciberseguridad en las empresas.

Propuesta

a. Para el planteamiento de estrategias para acelerar la formación de la fuerza laboral en ciberseguridad se retoman las recomendaciones presentadas en el marco del Reporte sobre el Desarrollo de Fuerza Laboral de Ciberseguridad, publicado en 2023 por la Organización de los Estados Americanos (OEA), la Comisión Interamericana de Cultura (CIC) y CISCO, particularmente:

1. Promover la recopilación y evaluación continua de datos del mercado y la fuerza laboral sobre ciberseguridad. Cubrir el déficit en el mercado laboral de ciberseguridad requiere un conocimiento detallado de la fuerza laboral en México. Por ello, es necesario que se impulse la recopilación de información y se promueva el análisis de las necesidades del mercado de la ciberseguridad y las tendencias relacionadas, a través de la identificación de métricas que muestren el alcance del problema y las posibles medidas para hacerle frente.
2. Para poder generar datos sobre el mercado laboral de ciberseguridad que permitan conocer en qué áreas en particular existen los mayores déficits en materia de fuerza laboral y desarrollar estrategias a la medida, es necesario contar con definiciones en común de los perfiles que requiere una organización para conformar los equipos o áreas de ciberseguridad. Asimismo, es importante homologar las definiciones en torno a las habilidades y capacidades para ejercer labores de ciberseguridad en la organización. Es importante que México cuente con un marco de definiciones de los roles, competencias, habilidades y conocimientos para facilitar la coordinación entre la industria y la formación profesional y académica, y asegurar que los egresados de programas universitarios relevantes cuenten con las habilidades requeridas por las empresas. Una buena referencia es el Marco Europeo de Habilidades en Ciberseguridad desarrollado por ENISA, que brinda una clasificación común de los diversos tipos de habilidades en materia de ciberseguridad. La publicación de una taxonomía común podría ser tarea de una Agencia Nacional de Ciberseguridad. Una guía que posiblemente se podría replicar y adaptar en México para la temática de ciberseguridad es el Marco de Habilidades Digitales para la Inclusión de la Secretaría de Infraestructura, Comunicaciones y Transportes (SICT), que incluye conceptualizaciones sobre el tipo Habilidades Digitales basadas en necesidades de inclusión de la sociedad, con énfasis en las necesidades del mercado y las habilidades requeridas por los empleadores de México y el mundo (SICT, 2019).
3. Crear una plataforma de coordinación entre actores de la industria e instituciones educativas para asegurar la compatibilidad entre los conocimientos y herramientas adquiridas en los planes de estudios con las necesidades de la industria en materia de ciberseguridad. Contar con esta plataforma de coordinación continua resulta particularmente importante ante la velocidad con la que avanza la innovación tecnológica en el sector digital, y las nuevas ciberamenazas que esto implica.
4. Aprovechar mejor el talento femenino para la ciberseguridad. Un grupo sub-representado en la ciberseguridad son las mujeres, que a nivel regional sólo representan un 24%

de la fuerza laboral de ciberseguridad (ASPENDIGITAL, 2021). Esto subraya el potencial de talento desaprovechado que existe todavía en este sector de la población. A su vez, dentro del sector privado ha crecido la conciencia sobre la importancia de aprovechar mejor el talento femenino para la ciberseguridad: a nivel mundial, el 70% de los gerentes de TI ven la contratación de mujeres como uno de los tres principales desafíos (FORTINET, 2022). En este sentido, resulta importante fortalecer la oferta de programas educativos dirigidos a niñas y mujeres de distintas edades. Entre los casos de éxito cabe mencionar las capacitaciones gratuitas que ofrece CISCO en Chile a mujeres bajo el Programa educacional de ciberseguridad Chilenas Conectadas y Seguras (OEA, 2023).

b. Las medidas que apuntan a la formación gradual de una fuerza laboral en materia de ciberseguridad se necesitan complementar con acciones que incrementen la resiliencia de PyMEs que, en muchos casos, no pueden costear uno de los escasos expertos en ciberseguridad. Con relación a esto se plantean las siguientes propuestas:

   1. En ausencia de expertos de ciberseguridad en muchas PyMEs, es de la mayor importancia que estas empresas puedan contar con guías prácticas alineadas a sus necesidades y recursos. Por ende, se propone recopilar en un sitio web centralizado un inventario de los recursos de capacitación: cursos en línea, talleres, y guías relevantes en el tema, disponibles en español y que apunten a facilitar el desarrollo de una política de ciberseguridad y la implementación de procesos de gestión de ciberseguridad en las empresas. En este inventario central se podrían incorporar o generar enlaces a los numerosos recursos que han sido desarrollados por diversas dependencias del Gobierno Federal para apoyar a las PyMEs en temas de ciberseguridad: las guías de ciberseguridad elaboradas por la SICT, incluida la Guía de Ciberseguridad para el uso seguro de las redes y dispositivos de telecomunicaciones en apoyo al teletrabajo, la plataforma MIPYMESMX de la Secretaría de Economía y el micrositio de Ciberseguridad del Instituto Federal de Telecomunicaciones (IFT). En este inventario, se sugiere además incluir metodologías para la gestión de riesgos entre las PyMEs. La gestión de riesgos generales es el punto de partida para una estrategia de ciberseguridad, ya que permite identificar los riesgos específicos que enfrenta cada empresa y, a partir de ello, definir estrategias de mitigación. Adicionalmente, se recomienda también incluir mapeos de los estándares internacionales más importantes en materia de ciberseguridad, así como de estándares del Instituto Nacional de Estándares y Tecnología (NIST) (que aplica a EE. UU.) y ENISA (que aplica a la UE), ya que el conocimiento de estos estándares resulta clave para las PyMEs que buscan integrarse a cadenas globales de valor y suministrar a multinacionales de otros países.
   2. En este mismo sitio web, proveer un inventario de proveedores de soluciones de ciberseguridad confiables, como antimalware, software para realizar análisis de vulnerabilidad, cifrados y sistemas de respaldos.
   3. En conjunto con aliados expertos, generar una herramienta de "checklist" de elementos estratégicos mínimos con los que deberían contar las PyMEs para mejorar su protección ante las ciberamenazas, en un lenguaje accesible y conciso. Este checklist deberá hacer referencia a los recursos mencionados en a) y el inventario de proveedores de soluciones en b) y estar dirigido al encargado de sistemas de las empresas como principal responsable de la ciberseguridad en las empresas que no cuentan con un experto.

4.4 Promover la certificación de empresas en ISO 27001 e IEC 63443

Antecedentes

Como se ha visto con antelación, en México ya se adoptaron los estándares internacionales de ciberseguridad ISO/IEC 27001 para SGSI, e IEC 62443 para la ciberseguridad industrial, bajo los nombres NMX-I-27001-NYCE-2015 y NMX-I-62443-4-1-NYCE-2021, correspondientemente.

Al tratarse de estándares internacionales elaborados por expertos y expertas de múltiples países y regiones, estos reúnen las mejores prácticas internacionales de vanguardia, además de que crean un marco de referencia común a nivel internacional, lo que facilita el reconocimiento transfronterizo de empresas certificadas y reduce barreras técnicas al comercio.

La adopción y certificación en ambos estándares va de la mano con múltiples beneficios para las empresas:

- Protección de datos: la certificación ayuda a las empresas a elevar el nivel de confianza sobre la protección de sus datos y los de sus clientes, lo que reduce el riesgo de brechas de seguridad.
- Confianza del cliente: las empresas certificadas pueden demostrar a sus clientes que tienen un SGSI robusto y eficaz. Esto puede aumentar la confianza del cliente y fortalecer la reputación de la empresa.
- Cumplimiento de la normativa: La certificación puede ayudar a las empresas a cumplir con las normativas nacionales e internacionales de protección de datos, evitando posibles sanciones.
- Mejora continua: el estándar internacional ISO/IEC 27001 fomenta la mejora continua de los procesos de gestión de la seguridad de la información, lo que puede conducir a una mayor eficiencia y eficacia.

© Biancoblue/Freepik

- Competitividad: en un mercado cada vez más globalizado, la certificación puede dar a las empresas una ventaja competitiva, en especial cuando se trata de conseguir contratos con grandes empresas o gobiernos que exigen este tipo de certificación. En muchos sectores particularmente vulnerables a ciberataques, para poder exportar a mercados como EE. UU. o la UE, ya se requiere contar incluso con una certificación en ISO 27001.

Empero, los bajos índices de certificación en estos estándares impiden que en la situación actual estos puedan contribuir de manera significativa a una mejora de las condiciones de ciberseguridad en el país. A su vez, implican una barrera en el desarrollo económico de pequeñas y medianas empresas que, al no contar con la certificación, enfrentan dificultades para integrarse a cadenas globales de valor.

Dadas las particularidades del contexto mexicano, resulta clave respaldar estos estándares con mecanismos de evaluación de la conformidad que brinden certidumbre de que la adopción de las prácticas de seguridad de la información y ciberseguridad reduce de manera efectiva los riesgos para la organización y su entorno. En la actualidad, muchas empresas hacen publicidad con el hecho de "estar alineados" con estos estándares. Sin embargo, es necesario que dichas empresas puedan ser evaluadas por una tercera parte para garantizar que sí están implementando los instrumentos que forman parte de estos estándares y generar confianza en sus posibles clientes.

Propuesta

Para lograr que los estándares de ciberseguridad que ya existen en México permeen de forma efectiva en el sector privado mexicano y puedan robustecer las condiciones de ciberseguridad de manera significativa, se sugieren tres áreas de acción complementarias. Estos esfuerzos se enfocan en promover la certificación en ISO 27001 o un estándar internacional comparable. En el caso de IEC 62443, se recomienda promover la adopción de este estándar de manera voluntaria entre las empresas del sector industrial.

1. Primero, se recomienda crear un catálogo de infraestructuras, servicios o actividades críticas que por su importancia sistémica y vulnerabilidad van a requerir la adopción y certificación de ISO 27001 o un estándar internacional comparable como la ISO/IEC 27103 basada en el NIST CSF. Entre estos destacan las actividades realizadas por las empresas del sector financiero, empresas de seguros, salud, y comunicaciones –debido a la sensibilidad de la información que manejan–, así como empresas involucradas en la infraestructura de energía y agua o las cadenas básicas de suministro –debido a su carácter sistémico-crítico–. En este tenor, la NMX-I-27001-NYCE-2015 o su equivalente correspondiente a la ISO/IEC 27001 se podría referenciar en una NOM aplicable a empresas en los sectores mencionados.
2. Al considerar que el mayor comprador en el país es el Gobierno, se propone además fomentar que se solicite a los proveedores y suministradores de servicios relacionados con servicios y tecnologías de información y comunicaciones para la administración Pública, la implementación y certificación en NMX-I-27001-NYCE-2015. De esta forma se podría comenzar a aumentar la demanda por empresas certificadas y los distintos niveles de gobierno pondrían un ejemplo a seguir. Este requisito se podría incorporar en el Acuerdo de la Administración Pública Federal 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 (APF). Este acuerdo establece que todos los proyectos institucionales que comprendan servicios e implementaciones tecnológicas y de seguridad de la información de la APF, deban acreditar los estándares o modelos reconocidos por el sector como mejores prácticas y cumplan con las normas oficiales.
3. Por otro lado, se sugiere complementar la recomendación 1) mediante la definición de exigencias verticales de mercado específicas asociadas con actividades transversales. Por ejemplo, para el procesamiento de datos personales que realizan empresas en distintos sectores. Una referencia para esta medida es Japón, donde toda empresa que procese datos personales para garantizar su protección tiene que estar certificada en el estándar ISO 27001. Una mayor exigencia de la certificación en NMX-I-27001-NYCE-2015 se podría implementar mediante la misma NOM mencionada en la recomendación 1), ampliada en su campo de aplicación por las empresas que realizan dichas actividades transversales.

Se sugiere que estas tres vías se implementen de manera gradual, comenzando con la implementación de estas propuestas en grandes empresas y avanzando hacia las medianas y pequeñas, conforme al avance en el desarrollo de las capacidades requeridas y el capital humano disponible. Para que estas propuestas puedan lograr un impacto significativo en mejorar la situación de ciberseguridad en el sector privado, deben estar acompañadas por programas que busquen fomentar las capacidades de empresas, particularmente PyMEs, la capacitación de su personal y la formación de expertos y expertas en materia de ciberseguridad como se especificó en 3.3.

Otra barrera importante que enfrentan las PyMEs con miras a procesos de certificación son los costos asociados con estos, tanto en la implementación de los lineamientos especificados en ISO 27001 en la organización,

como con la auditoría requerida para la certificación. Para no generar una dinámica de exclusión hacia las PyMEs, que hoy en día se enfrentan a la necesidad de certificarse en ISO 27001 e IEC 62443 como exigencia de los mercados internacionales, se podría contemplar el desarrollo de programas que brinden recursos técnicos, humanos y de otra índole para hacer asequible la certificación de PyMEs en estándares relevantes.

4.5 Adoptar otros estándares internacionales complementarios a ISO 27001 e IEC 62443

Antecedentes

Es importante resaltar que el estándar ISO/IEC 27001 adoptado para el contexto mexicano es un estándar genérico que enmarca toda una familia de estándares ISO/IEC 27000. Los otros estándares de la serie incluyen soluciones técnicas detalladas para actividades particulares dentro de la ciberseguridad como la gestión de incidentes (ISO/IEC 27035), la detección de incidentes (ISO/IEC 27039) o la seguridad de la información en las relaciones con proveedores (ISO 27036), así como aplicaciones de ISO/IEC 27000 a sectores específicos, como telecomunicaciones, energía y salud.

En este sentido, resulta importante avanzar hacia la adopción de otros estándares de la familia, considerando también su función de transferencia tecnológica y las soluciones técnicas detalladas que ofrecen los demás estándares de la serie ISO 27000.

También existen estándares internacionales y regionales en otras partes del mundo enfocados al internet de las cosas, inteligencia artificial y temas relacionados que pueden abonar, por ejemplo:

- ENISA Guidelines for securing internet of things.
- EN 303 645 - V2.1.0 - CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements.
- ISO/IEC CD 27402.2 Cybersecurity — IoT security and privacy — Device baseline requirements.
- ISO/IEC WD 27403.6 Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics.

Propuesta

En cuanto se avance con la implementación de los estándares ya referenciados (IEC 62443 e ISO/IEC 27001) y se logre un incremento en la proporción de empresas certificadas, tal como se expone en la propuesta 4), la recomendación es revisar la adopción de otros estándares de la serie ISO 27000. La priorización de estándares a adoptar de esta familia debe ser resultado de un análisis de la situación de las empresas en asuntos de ciberseguridad en México (propuesta 1), que identifique industrias y/o actividades que sean más vulnerables. Se recomienda que aquí se consideren de manera concreta los estándares mencionados para el internet de las cosas e inteligencia artificial, dada su fuerte presencia en México en los sectores financiero, de salud, energía, transporte, alimentos y entretenimiento.

5. Conclusión

// En este documento se presentaron cinco recomendaciones para fortalecer la ciberseguridad en el sector privado mexicano. México ha sido uno de los países más atacados por ciberdelincuentes, con 80,000 millones de intentos de ciberataques tan sólo en el primer trimestre de 2022. Un segmento particularmente vulnerable en el sector privado han sido las PyMEs, que constituyen una fuente importante de empleo en el país. Las condiciones en este tipo de empresas son tales que un 86% de ellas no se encuentra preparada para las ciberamenazas que hoy existen.

© Lovephoto/Freepik

La brecha entre el veloz desarrollo de ciberamenazas sin fronteras, y el insuficiente nivel de implementación de estrategias de ciberseguridad y herramientas de protección genera una fuerte necesidad de acciones coordinadas entre el sector público y privado que apunten a robustecer las condiciones de ciberseguridad en las empresas. La implementación de estándares internacionales en materia de ciberseguridad, que reúnen conocimientos y procesos de vanguardia y son actualizados con regularidad, y el fomento de capacidades en las empresas, son pilares fundamentales para este fin. Estos pilares guían las recomendaciones recabadas en el presente documento.

Las recomendaciones incluyen:

1. Realizar un mapeo del estado de madurez en lo relativo a ciberseguridad en las empresas que operan en México.
2. Fomentar la cooperación regulatoria internacional en materia de ciberseguridad.
3. Fortalecer las capacidades de ciberseguridad en a) el personal y b) las políticas y procesos de gestión de ciberseguridad de las empresas.
4. Generar y promover incentivos y mecanismos para que, de manera gradual, una mayor cantidad de PyMEs en el país pueda certificarse en la ISO 27001, con particular énfasis en sectores críticos.
5. Adoptar otros estándares internacionales complementarios a ISO 27001 e IEC 62443 para ponerlos a disposición de empresas mexicanas.

Estas recomendaciones interdependientes constituyen un conjunto de acciones estratégicas que apuntan al desarrollo de capacidades a nivel individual y a nivel empresa, y buscan fortalecer el marco regulatorio para este fin. Por su interdependencia, se considera que estos elementos podrían ser coordinados y monitoreados por un organismo centralizado como la Agencia Nacional de Ciberseguridad que se ha incluido en algunas propuestas de Ley de Ciberseguridad. Al mismo tiempo, dada la diversidad de características y actividades de empresas, es necesario que los elementos de esta estrategia sean traducidos en actividades diferenciadas, de acuerdo los niveles de madurez en materia de ciberseguridad y la importancia sistémica de distintos segmentos del sector privado.

6. Referencias

[1] ASPENDIGITAL. (2021). Diversity, Equity, and Inclusion in Cybersecurity.

[2] Congreso de la Unión (2010). Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Cámara de Diputados.

[3] Deloitte (2020). Consideraciones de Ciberseguridad en medio de una pandemia global. Deloitte.

[4] Forbes (29 de junio de 2020). Pymes, las más vulnerables ante la ciberdelincuencia. Forbes.

[5] Forbes (2 de agosto de 2022). México registra 80,000 millones de intentos de ciberataques en 2022. Forbes.

[6] FORTINET. (2022). 2022 Cybersecurity Skills Gap - Global Research Report.

[7] Hernández, G. (12 de octubre de 2022). Especialistas en ciberseguridad, talento escaso y cada vez más peleado por las empresas. El Economista.

[8] International Electrotechnical Commission (2021). Understanding IEC 62443. IEC blog.

[9] International Organization for Standardization (2022a). Information Security Management Systems. ISO.

[10] International Organization for Standardization (2022b). ISO Survey Report 2022. ISO.

[11] Organización de los Estados Americanos (2023). Reporte sobre el desarrollo de la fuerza laboral de ciberseguridad en una era de escasez de talento y habilidades. OEA.

[12] Olivera, S. (18 de abril de 2023). La PyMe en México en la mira de los hackers, ¿cómo enfrentar esta amenaza? eSemanal.

[13] Senado de la República (29 de febrero de 2020). Pymes, importante motor para el desarrollo económico nacional: MC. Boletines.

[14] Secretaría de Infraestructura, Comunicaciones y Transportes (2019). Marco de Habilidades Digitales para la inclusión. SICT.

[15] Zamarrón, I. (18 de enero de 2023). Un ciberataque le puede costar 2 mdp a una pyme, además del daño reputacional. Forbes.