Importancia de la Ciberseguridad en la transformación digital de las empresas

GPQI
Dialogues for Innovation and Trade

Publicado por
Deutsche Gesellschaft für
Internationale Zusammenarbeit (GIZ) GmbH

Oficinas registradas
Bonn and Eschborn, Germany

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

Diseño
Kathrin von Eye

Créditos fotográficos
Título: Michael Traitovo/Shutterstock

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 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

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 primero de cuatro volúmenes que aborda la importancia de la ciberseguridad en las Micro, Pequeñas y Medianas Empresas (MiPyMEs), así como el papel que tiene el uso de estándares armonizados a nivel global en 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.

Descargo de responsabilidad: Este documento, creado por un grupo bilateral de expertos, se proporciona con fines informativos, de forma gratuita y no será vendido como una publicación comercial. No representa la posición oficial de la Secretaría de Economía de México ni del Ministerio Federal de Economía y Protección del Clima (BMWK) de Alemania. Esta declaración también se aplica a la Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH, que opera en nombre del BMWK. Aunque se ha tenido cuidado en la elaboración de los contenidos, que se han preparado de buena fe sobre la base de la información disponible en la fecha de publicación sin verificación independiente, la GIZ no garantiza ni respalda la precisión, confiabilidad, integridad o actualidad de la información en esta publicación.

Contenido

1. Introducción: contexto de la seguridad de la información, la ciberseguridad y el cibercrimen

// La transformación digital es quizás una de las evoluciones tecnológicas más importantes en la historia moderna. La cantidad de datos generados en cualquier proceso productivo no tiene precedentes. En los últimos años, se ha presentado una tendencia generalizada y creciente a la digitalización en casi todos los sectores de la industria a nivel global, impulsada en gran medida en los últimos años por la pandemia de COVID-19 y la necesidad de los negocios de adaptarse para hacer frente a los nuevos desafíos planteados por esta situación.

© metamorworks/Shutterstock

Por otra parte, cada vez son más los negocios que ofrecen modelos de trabajo mixtos que combinan el trabajo en oficina y el teletrabajo. Estos cambios en la forma de trabajar han creado nuevos riesgos de ciberseguridad y vulnerabilidades, porque la mayoría de las veces el nivel de ciberseguridad que se tiene en casa no es el mismo con el que se cuenta en las instalaciones de las empresas. Además, muchas personas se han visto en la necesidad de utilizar las tecnologías de la información sin tener ningún conocimiento en temas de ciberseguridad, lo cual ha significado una oportunidad para los cibercriminales de poder aprovecharse de las poblaciones más vulnerables.

Según la Cuarta Encuesta 2022 del Instituto Federal de Telecomunicaciones (IFT), llamada "Usuarios de servicios de telecomunicaciones (micro, pequeñas y medianas empresas)", las MiPyMEs han incrementado el uso de los servicios de telecomunicaciones. Un ejemplo de esto es el aumento en el uso del servicio de internet fijo por parte de las mismas. En el año 2021, el 73.6% de las empresas contrataron este servicio, mientras que en 2022 ese porcentaje aumentó a un 79.9%, siendo las pequeñas y medianas empresas las que experimentaron un mayor crecimiento en la contratación de este servicio.[1]

Así como la tecnología y su uso han evolucionado en los últimos tiempos, también lo han hecho las amenazas relacionadas con la creación y diseminación de programas de software maliciosos. Hemos pasado de los primeros virus, gusanos, troyanos y puertas traseras que infectan los equipos de cómputo, a diversos tipos de *malware*, como los que buscan afectar infraestructuras críticas como *Stuxnet* o *Industroyer*; software espía que pretende robar información confidencial o propiedad intelectual de sus víctimas; *ransomware*, que busca obtener beneficios económicos al secuestrar la información contenida en los equipos de sus víctimas; o el *killware*, que pone en riesgo la vida humana.[2]

La industria del cibercrimen ha registrado un crecimiento del 600% desde el comienzo de la pandemia y se estima que para el año 2025 el costo del cibercrimen para las organizaciones será de alrededor de 10.5 billones de dólares anuales, convirtiéndola en uno de los negocios más rentables y superando incluso a otros negocios ilegales, como el narcotráfico[3]. Algunas de las afectaciones que el cibercrimen puede generar son daño y destrucción de datos, extorsión económica, pérdida de productividad, robo de propiedad intelectual, robo de datos personales y financieros, malversación de fondos, fraude, interrupción de la continuidad de los negocios, daño a la reputación de las empresas, interrupción en los procesos productivos, etc.

// ASÍ COMO LA TECNOLOGÍA Y SU USO HAN EVOLUCIONADO EN LOS ÚLTIMOS TIEMPOS, TAMBIÉN LO HAN HECHO LAS AMENAZAS RELACIONADAS CON LA CREACIÓN Y DISEMINACIÓN DE PROGRAMAS DE SOFTWARE MALICIOSOS. //

En el año 2020 los ataques con algún tipo de *malware* y *ransomware* se incrementaron a nivel global en un 358% y 435%, respectivamente.[4] De hecho, se considera al *ransomware* como la amenaza emergente que más pone en riesgo la continuidad de los negocios. También en ese año se registraron 4,000 ataques diarios a nivel mundial que tuvieron un costo de 350 millones de dólares para las víctimas, mientras que el 92% de las empresas que pagaron el rescate en 2021 no recuperaron su información.[5] Por otra parte, el *ransomware* como servicio ha permitido que criminales sin conocimientos técnicos puedan realizar ciberataques que no sólo se limitan al cifrado de los datos, sino que amenazan a las víctimas con filtrar la información robada antes de cifrarla y con efectuar ataques distribuidos de Denegación de Servicio[6] a su infraestructura.[7]

El informe "Panorama de Amenazas en América Latina 2022" de la firma Kaspersky muestra que en los primeros ocho meses de 2022 las tecnologías de la empresa bloquearon 38 millones de accesos a enlaces fraudulentos, cifra que representa el 75% de los intentos de *phishing* de 2021, cuando se registraron un total de 52 millones. En promedio, Kaspersky evita 110 visitas fraudulentas a sitios web por minuto en la región.[8]

En América Latina, México ocupa el tercer lugar en ciberataques con 1.7 millones de intentos en 2021, tan sólo detrás de Brasil con más de 5 millones y Colombia con 1.8 millones. Además, según un estudio de Deloitte,[9] el 62% de las empresas en México han sufrido ciberataques desde el inicio de la pandemia y al menos el 76% han sufrido uno o dos ataques significativos al año.

De acuerdo con el Índice Global de Ciberseguridad de la Unión Internacional de Telecomunicaciones (UIT) 2020, que mide el compromiso de sus estados miembro con la ciberseguridad a través de las medidas jurídicas, técnicas, institucionales, de capacitación y cooperación implementadas, en 2020 México alcanzó el lugar 52 de 194 naciones consideradas en el estudio, 11 lugares arriba respecto al año 2018.[10] Sin embargo, aún existe un largo camino por recorrer en todo el país de cara a este nuevo entorno híper digital.

Según el "Informe de Riesgos Globales" emitido por el Foro Económico Mundial en su 17ª edición, uno de los principales riesgos tecnológicos a los que se enfrenta la humanidad son las "fallas de ciberseguridad", cuya principal causa son el incremento de las vulnerabilidades que presenta la tecnología y que no son corregidas a tiempo, siendo entonces explotadas por los cibercriminales. Por ejemplo, en diciembre de 2021, tan sólo una semana después del descubrimiento de una vulnerabilidad crítica[11] en una librería altamente utilizada de Java (Log4j) se registraron más de 100 intentos de explotación de dicha vulnerabilidad por minuto en todo el mundo.[12]

Una de las causas por las que se presentan estas "fallas de ciberseguridad" a nivel organizacional es la falta de una cultura de ciberseguridad, lo que ha generado que 95% de los problemas en la materia sean originados por algún error de tipo humano, mientras que el 43% de todas las brechas[13] reportadas se debieron a amenazas internas (intencionales o accidentales). De igual forma, afecta la falta de profesionales en ciberseguridad que hay en el mercado y cuyo déficit se calcula en 3 millones a nivel global. [14]

Adicionalmente, existe una creciente preocupación por el uso de tecnologías emergentes que pudieran poner en riesgo la seguridad de la información debido a las nuevas oportunidades que ofrecen a los cibercriminales. Destaca, por ejemplo, la computación cuántica,[15] la cual podría ser tan poderosa como para romper las llaves de cifrado empleadas para proteger datos sensibles. También están las *deepfakes*, técnicas de inteligencia artificial que permiten crear fotografías o videos falsos de personas que aparentan ser reales, o la „desinformación por encargo", que podría ser utilizada para manipular e influir en las decisiones de las personas o incluso emplearse para llevar a cabo fraudes. Fue así como hace poco los ciberdelincuentes clonaron la voz de un director de empresa para autorizar la transferencia de 35 millones de dólares a cuentas fraudulentas.[16] Situaciones como las anteriores ponen de manifiesto la necesidad de realizar esfuerzos internacionales entre los distintos gobiernos para lograr una mitigación de riesgos.

En línea con lo recién expuesto sobre los sucesos de los últimos años, el Foro Económico Mundial ha incluido en la última edición del "Informe de Riesgos Globales 2023" a la ciberdelincuencia y la inseguridad cibernética en el ranking de los 10 riesgos más severos sobre la próxima década a nivel global.[17] Lo anterior ratifica la importancia de esta situación no sólo por su impacto, sino por su tendencia a crecer en complejidad y sofisticación, así como por su presencia en sectores de la sociedad que tradicionalmente no eran afectados por temas de ciberseguridad como, por ejemplo, las MiPyMEs, que dejaron de hacer comercio tradicional y comenzaron a realizar transacciones por medio del comercio electrónico.

2. Conceptos

// En toda empresa los activos deben ser gestionados de manera apropiada por su valor e impacto en las operaciones del negocio. En el contexto de la transformación digital, la gestión de la información es vital; por lo que es crucial entender los conceptos básicos que permitan a las empresas identificar sus necesidades en cuanto a la gestión de información, así como conocer los **riesgos inherentes a la transformación digital de sus procesos**.

© U-STUDIOGRAPHY DD59/Shutterstock

Seguridad de la información y ciberseguridad

Estos términos se utilizan a menudo de forma errónea porque son casi sinónimos. Tanto la seguridad de la información como la ciberseguridad se definen como la práctica de defender la información ante un acceso, uso, modificación o interrupción no autorizado. La única diferencia entre ambas está en la forma de los datos: mientras que la ciberseguridad serefiere únicamente a la seguridad electrónica, la seguridad de la información es un término más amplio que abarca todos los datos, tanto físicos como digitales.

¿Qué es la ciberseguridad?

La ciberseguridad es la prevención del daño, la protección y la restauración de computadoras, sistemas de comunicaciones electrónicas, servicios de comunicaciones electrónicas, comunicaciones fijas y comunicación electrónica, incluyendo la información contenida en ellas, para garantizar su disponibilidad, integridad, autenticación, confidencialidad y no repudio.[18]

También puede entenderse como el conjunto de herramientas, políticas, conceptos, acciones, prácticas idóneas y tecnologías que pueden utilizarse para proteger a los usuarios, sus dispositivos y la información transmitida y/o almacenada de los riesgos de seguridad que hay en el ciberentorno.[19]

¿Qué es la seguridad de la información?

De acuerdo con la International Organization for Standardization (ISO), la seguridad de la información es la preservación de la confidencialidad, integridad y disponibilidad de la información.[20]

La seguridad de la información es un conjunto de medidas técnicas, organizativas y legales que permiten a una organización salvaguardar la confidencialidad, integridad y disponibilidad de la información.[21] Implica la protección de la información y los sistemas de información de accesos sin autorización, uso, revelación, disrupción, modificación o destrucción para preservar dichos elementos, entre ellos:

- **Autenticidad.** Característica de la información que refiere a que esta es válida y utilizable en tiempo, forma y distribución. Esta propiedad permite asegurar el origen de la información, validando el emisor, el receptor o ambos.[22]
- **Confidencialidad.** Confidencialidad. Se refiere a que la información sólo debe ser conocida por las personas autorizadas.
- **Integridad.** Es la característica de la información que hace que su contenido permanezca inalterado a menos que sea modificado por personal o procesos autorizados; dicha modificación debe ser registrada para controles o revisiones posteriores.[23]
- **Disponibilidad.** Es la capacidad que tiene la información de poder ser usada en cualquier momento para ser procesada por las personas autorizadas; esto requiere su correcto almacenamiento y que el software y hardware para su consulta y posterior procesamiento funcionen en condiciones óptimas.[24]

¿Qué es una amenaza?

En materia de seguridad de la información se emplea el término "amenaza" para señalar una acción tendiente a causar un daño a los dispositivos o sistemas en donde se encuentra almacenada la información, atentando contra su confidencialidad, integridad y disponibilidad.[25] En estos términos, si una amenaza se llega a concretar, surgirán diversas consecuencias como, por ejemplo, interrupción de un servicio o procesamiento de un sistema, modificación o eliminación de la información, daños físicos, robo del equipo y medios de almacenamiento de la información, entre otros. Las amenazas a la seguridad informática se clasifican en humanas, lógicas y físicas e infraestructura crítica *(safety).*

Las amenazas cibernéticas y los incidentes son un riesgo operativo y comercial muy importante para todas las empresas, especialmente aquellas que se encuentren en procesos de transformación digital. En la era de la digitalización es fundamental crear y ejecutar estrategias que permitan a las organizaciones identificar, proteger, detectar, responder y recuperar sus activos tecnológicos ante las diferentes amenazas y riesgos cibernéticos que enfrentan, para asegurar sus operaciones y alcanzar sus objetivos financieros.

3. Transformación digital y ciberseguridad en las empresas

// La transformación digital es el proceso en el que las empresas adoptan tecnologías digitales en diversas áreas que forman parte del negocio para conseguir cambios y beneficios en diferentes aspectos, como incrementar la eficiencia, aumentar la producción, conseguir agilidad en sus operaciones, desbloquear o propiciar nuevas habilidades en su personal, alcanzar un mayor número de clientes o mejorar la relación con los mismos.

Ahora bien, las mejores prácticas internacionales indican que la adopción de nuevas tecnologías debe realizarse con base en una estrategia de transformación digital, la cual debe ser ampliamente planificada y parte integral de la estrategia general de la empresa; es decir, debe alinearse con los objetivos, misión y visión de la organización. Asimismo, debe tener una estructura operacional adecuada y suficiente, recursos dedicados y una clara definición de objetivos específicos, entre otros. En resumen, la transformación digital debe ser un esfuerzo integral de toda la empresa basado en la tecnología, las personas y los procesos que habiliten dicho proceso de cambio.

Más allá del aspecto tecnológico, la estrategia de transformación digital debe gestionar de manera adecuada los riesgos y las oportunidades derivadas de este proceso de cambio. En este sentido, las amenazas cibernéticas son uno de los elementos más importantes que debe considerar una estrategia de transformación digital y debe formar parte de sus objetivos, para así aprovechar los beneficios de la transformación digital; por tanto, dichas amenazas deben ser abordadas de manera estratégica dada su creciente ocurrencia y alto impacto.

Es importante indicar que abordar el tema de ciberseguridad en una empresa no consiste únicamente de invertir en tecnología de punta sólo por ser tendencia o porque dicha tecnología "promete" eliminar todos los ciber riesgos. Tampoco se trata de implementar políticas altamente restrictivas con el objetivo de eliminar las condiciones de riesgo, ya que ello podría incluso afectar la operatividad y agilidad de la empresa. Por el contrario, el tema debe ser abordado de manera estructurada a través de una estrategia de ciberseguridad sólida, de carácter multidimensional y transversal que considere los aspectos y elementos más críticos de la operación de la empresa, protegiéndolos bajo un concepto multicapa (concepto "Defense in Depth"[26]), tal como lo recomiendan los estándares internacionales como el IEC[27] 62443, y considerando la competencia del recurso humano disponible, la incidencia en procesos internos y el uso eficiente de las diferentes tecnologías disponibles.

Uno de los elementos habilitadores del proceso de cambio que representa la transformación digital es, sin duda, el factor humano. Antes se comentó sobre la importancia de contar con el apoyo de la alta dirección; sin embargo, aunado a esto se requiere el involucramiento de actores clave que aporten diferentes perspectivas, conocimientos y habilidades. Ahora bien, lo recomendable es que dichos actores estén organizados de tal manera que puedan abarcar las diferentes áreas y niveles de la organización sin que los esfuerzos se dupliquen o, incluso, lleguen a colisionar. Para esto es importante que el responsable de liderar la transformación digital habilite –en la medida de las necesidades de la organización– una estructura organizacional plana, adaptable y transversal que permita el cambio sostenible; una estructura con responsables tecnológicos (IT & OT), responsables financieros, agentes de recursos humanos y líderes de grupo que puedan traer y llevar las opiniones del personal operativo hacia aquellos que desarrollan e implementan la estrategia.

4. Industria 4.0: la transformación digital en el ámbito industrial

// El proceso de transformación digital ha alcanzado prácticamente toda actividad económica, desde el sector primario –como la extracción y producción de materias primas (alimentos, minerales)–, pasando por actividades secundarias como la construcción, generación, transporte de energía y casi toda industria de transformación y, por último, el grupo terciario enfocado en proveer servicios a consumidores finales, donde podemos encontrar todo tipo de comercio, turismo, transporte, salud y servicios financieros.

Si bien cada uno de los participantes de estas actividades económicas tiene sus propios retos en el proceso de transformación digital, entre ellos existe un grupo cuyas características particulares hacen de su proceso de adopción de nuevas tecnologías un elemento crítico para subsistir y ser relevante en el mercado y ambiente que se desarrolla. Hablamos de la industria de la manufactura,[28] la cual en México aporta alrededor del 17%[29] del Producto Interno Bruto, además de emplear a casi 9 millones de personas en el país.

La industria manufacturera, especialmente las pequeñas y medianas empresas (PyMEs), enfrenta muchos retos durante su transformación digital. Esto se da tanto en el aspecto tecnológico, como en el operacional de la empresa.

© Blue Planet Studio/Shutterstock

Algunos de los aspectos tecnológicos a los que se enfrentan la mayoría son:

- Falta de modernización en su infraestructura operativa.
- Base instalada multimarca.
- Redes de comunicación no gestionadas.
- Sistemas obsoletos, cerrados o incompatibles con otros sistemas.
- Conocimiento técnico limitado en su personal.

A diferencia de los retos tecnológicos –los cuales pueden ser superados por las empresas con la ayuda de socios tecnológicos, capital y planeación–, los aspectos operacionales implican cuestiones más complejas, como la cultura organizacional, la resistencia al cambio y la adaptabilidad del personal. A continuación, se enlistan algunos ejemplos de los retos que se identifican en las empresas, además de los asociados con la tecnología:

// LOS RETOS OPERACIONALES IMPLICAN CUESTIONES COMPLEJAS COMO LA CULTURA ORGANIZACIONAL, LA RESISTENCIA AL CAMBIO Y LA ADAPTABILIDAD DEL PERSONAL. //

- Poca planeación de crecimiento en infraestructura.
- Falta de procesos que describan correctamente las operaciones.
- Resistencia al cambio tecnológico en áreas productivas.
- Falta de cultura orientada a la seguridad de la información y la ciberseguridad.
- Mano de obra no calificada para el manejo de sistemas más avanzados.
- Falta de estrategias sólidas de transformación digital y ciberseguridad.
- Poca atención de la alta dirección en temas de transformación y ciberseguridad.
- Presupuestos reducidos para renovación tecnológica.
- Procesos manuales poco eficientes o de poco valor.
- Falta de procesos y sistemas de gestión en la empresa.
- Falta de conciencia del personal con respecto a la ciberseguridad.

Es un hecho que, según información de múltiples organizaciones como el Foro Económico Mundial en su "Informe de Riesgos Globales 2022"[30] o la empresa Kaspersky en un informe sobre ciberamenazas en Sistemas de Control Industrial,[31] el número de ciberataques en Latinoamérica–especialmente en el sector industrial– no sólo ha aumentado en número sino en complejidad, alcanzando no sólo a empresas trasnacionales o mega-sitios de producción, sino que los objetivos de los atacantes son de lo más variados en sofisticación, tipo de industria y tamaño de empresas. Se ha identificado que esta tendencia seguirá creciendo en los siguientes años, por lo que constituye uno de los riesgos globales más importantes para la sociedad.

Si a esta situación se le añaden algunos de los factores antes mencionados, tales como la obsolescencia de equipos y sistemas de producción, la falta de conciencia y conocimiento del tema entre los empleados, o la falta de inversiones en ciberseguridad con enfoque preventivo, entonces tenemos como consecuencia un ambiente de alto riesgo en el que existirán *gaps* tecnológicos, vulnerabilidades y prácticas inseguras que pueden ser explotadas por los ciberatacantes y tener consecuencias muy importantes en términos económicos, así como de seguridad para los empleados o el medio ambiente.

Por todo lo anterior, en el contexto actual de la transformación digital es fundamental que las empresas diseñen, implementen, adopten y actualicen planes y protocolos de ciberseguridad. Estas medidas son esenciales para prevenir posibles ciberataques, así como para gestionar de manera eficiente cualquier contingencia que pueda surgir. Asimismo, contar con un enfoque proactivo en ciberseguridad garantiza la continuidad de las operaciones y protege la información confidencial de la empresa y de sus clientes. Lo ideal es que estas estrategias tomen como referencia los estándares internacionales, como ISO/IEC 62443, que tienen apartados y recomendaciones específicas para cada aspecto de la empresa y, de manera particular, para la protección de sistemas de control de la industria manufacturera.

5. Cadenas de suministro conectadas

© ZinetroN/Shutterstock

// Una de las características y propósitos de la digitalización es crear transparencia operativa a través de interconectar elementos de campo que generan datos para convertirlos en información útil. Dichos elementos englobarían motores, líneas de ensamblaje, medidores de energía y otros más que provean información de primera mano y que, con ayuda de procesamiento y análisis, permitan tomar decisiones que favorezcan las operaciones de la empresa.

Si analizamos esto en una escala mayor, existe una interdependencia de las diferentes empresas productoras de materia prima, productos y servicios intermedios y productos para consumo final. Esta interdependencia, conocida como cadena de suministro, debe ser gestionada de manera ordenada y coordinada para asegurar la producción eficiente y, con ello, traer beneficios a cada uno de sus participantes, incluyendo a los consumidores finales. En este sentido, la digitalización busca ayudar a estas estructuras a través de la transparencia de datos, el análisis de grandes cantidades de datos y tendencias, la interconectividad de sistemas de producción, etc., todo ello con el mismo objetivo: generar información relevante para los procesos de toma de decisión.

No obstante, si bien contar con empresas conectadas, intercambio de datos, y sistemas administrativos y de producción interconectados son factores que buscan generar beneficios para las empresas, también traen consigo mayores riesgos. Tener políticas de ciberseguridad dentro de una empresa puede llegar a ser un esfuerzo complejo; tenerlas a lo largo de varias empresas de distintos tamaños, niveles de automatización, diversidad de culturas organizacionales, distintos niveles de madurez en procesos, etc., lo hace aún más complicado. Sin embargo, si cada una de estas define políticas de ciberseguridad alineadas a los estándares internacionales, será bastante más sencillo encontrar puntos comunes (controles, procesos, competencias) que permitan la coordinación de esfuerzos, así como la compartición de experiencias, mejores prácticas y recursos de distintos actores relevantes del ecosistema digital. Todo ello encaminado a la protección de toda la cadena de suministros en contra de ciberataques, desde la prevención hasta planes conjuntos de reacción y recuperación ante ataques.

6. Conclusión

// En resumen, los tomadores de decisión deben considerar que los riesgos de ciberseguridad siempre van a existir, sin importar el nivel de digitalización adoptado en su empresa. En este sentido, la ciberseguridad se concibe como un componente más de la transformación digital y como un habilitador para la adopción de nuevas tecnologías. A su vez, es importante que la empresa tome una postura resiliente durante su proceso de transformación pues el riesgo será permanente. Sin embargo, lo relevante es que las organizaciones estén preparadas para actuar antes de que dichos riesgos se materialicen para así evitar catástrofes en las empresas a nivel operacional, financiero, reputacional, etc.

Precisamente los estándares internacionales, tales como los publicados por ISO/IEC, incluyen apartados específicos sobre cómo las organizaciones deben definir los procesos de gestión de incidentes y vulnerabilidades, y cómo crear planes de recuperación tras ciber-incidentes. Así, estos estándares constituyen una gran herramienta que permite a las empresas diseñar estrategias y sistemas de gestión orientados a minimizar los riesgos de ciberseguridad a través de procesos bien definidos que involucren la generación de nuevas competencias entre el recurso humano de la empresa. Los estándares internacionales son una solución viable, validada y pensada justamente para hacer uso eficiente de los esfuerzos y los recursos de una empresa y obtener resultados.

// LOS ESTÁNDARES INTERNACIONALES SON UNA GRAN HERRAMIENTA QUE PERMITE A LAS EMPRESAS MINIMIZAR LOS RIESGOS DE CIBERSEGURIDAD. //

En este sentido, dos de los estándares internacionales que ayudan a las empresas a aprovechar de mejor manera sus recursos son los estándares de la serie ISO/IEC 27000 enfocados en la seguridad de la información, así como IEC 62443 orientado a la ciberseguridad en el ámbito industrial. Ambos tienen un enfoque en la gestión de riesgos no sólo tecnológicos sino organizacionales, así como en la mejora continua de procesos.

Estos dos estándares, y algunos otros, serán abordados con mayor detalle en el documento "Los estándares internacionales y el fortalecimiento de la ciberseguridad en la industria", el cual es el segundo documento del grupo de trabajo sobre "Ciberseguridad en el contexto de la digitalización y la Industria 4.0".

7. Referencias

[1] Instituto Federal de Telecomunicaciones — IFT. (2022). Cuarta encuesta 2022, usuarios de servicios de telecomunicaciones.

[2] Saengphaibul, V. (2022). A Brief history of the evolution of malware.

[3] Morgan, S. (2020). Cybercrime to Cost the World $10.5 Trillion Annually by 2025.

[4] World Economic Forum. (2022). The Global Risks Report 2022.

[5] Deloitte. (2022). Cyber Security Landscape 2022.

[6] Se trata de un intento malintencionado de afectar la disponibilidad de un sistema (sitio web, aplicación, plataforma o dispositivo) con el fin de bloquear su servicio. Este tipo de ataque puede afectar tanto a la fuente que ofrece la información, como a la red informática. Existen dos técnicas muy utilizadas para concretar este tipo de ataques: la denegación de servicio o Denial of Service (DoS, por sus siglas en inglés) y la denegación de servicio distribuido o Distributed Denial of Service (DDoS, por sus siglas en inglés). Para más información consultar: Oficina de Seguridad del Internauta (INCIBE). ¿Qué son los ataques DoS y DDoS? Instituto Nacional de Ciberseguridad es ciberse guridad — INCIBE. (2018).

[7] ¿Qué son los ataques DoS y DDoS?.

[8] World Economic Forum. (2022). The Global Risks Report 2022.

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

[10] Kaspersky. (2022). Los ataques financieros crecen en América Latina y aumenta la preocupación por el uso de la piratería.

[11] Riquelme, R. (2021). México avanzó 11 lugares en Índice Global de Ciberseguridad de la ITU, pero le falta estrategia y regulación.

[12] Una vulnerabilidad informática se refiere a una falla o error en el código de un sistema o dispositivo que, cuando se aprovecha, puede comprometer la seguridad de la información personal o de una organización. En este contexto, una vulnerabilidad crítica es la peor forma de vulnerabilidad, ya que se propaga sin la necesidad de la intervención de los usuarios. Esto pone en peligro la confidencialidad, disponibilidad e integridad de los datos de los usuarios, así como la integridad y disponibilidad de los recursos del sistema. Limones, E. (2022). Análisis de vulnerabilidades informáticas.

[13] Riquelme, R. (2021). México avanzó 11 lugares en Índice Global de Ciberseguridad de la ITU, pero le falta estrategia y regulación.

[14] Una brecha de ciberseguridad es un evento que permite el acceso no autorizado a datos informáticos, aplicaciones, redes o dispositivos. En otras palabras, permite acceder a la información sin tener permiso. Por lo general, ocurre cuando un intruso logra evadir los sistemas de seguridad establecidos. Kaspersky. (s.f.). ¿Qué es una brecha de seguridad?

[15] Riquelme, R. (2021). México avanzó 11 lugares en Índice Global de Ciberseguridad de la ITU, pero le falta estrategia y regulación.

[16] La computación cuántica se basa en los principios de la mecánica cuántica y es una forma de procesamiento de información. En lugar de utilizar bits, como en la computación clásica, se utilizan cúbits ("qubits" en inglés) para procesar la información. Mientras que los bits sólo pueden ser 0 o 1, los qubits pueden ser 0, 1 o ambos al mismo tiempo. La computación cuántica combina disciplinas como ciencias de la computación, física y matemáticas, y aprovecha los aspectos de la mecánica cuántica para resolver problemas complejos que las computadoras tradicionales no pueden abordar. A diferencia de la computación clásica, la computación cuántica se caracteriza por su mayor capacidad de cálculo, su capacidad de memoria y su menor consumo de energía. Centro México Digital. (2023). ¿Qué es la Computación Cuántica y cuáles son sus ventajas y desventajas?

[17] Riquelme, R. (2021). México avanzó 11 lugares en Índice Global de Ciberseguridad de la ITU, pero le falta estrategia y regulación.

[18] World Economic Forum (2023). The Global Risks Report 2023.

[19] National Institute of Standards and Technology — NIST. (s.f.). Glossary of Key Information Security Terms.

[20] IFT. (s.f.). Glosario de Ciberseguridad.

[21] International Organization for Standardization — ISO. (2022). ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection.

[22] Bernuy, J. (2008). Implementación de seguridad de la información mediante ISO-17799 plataforma BSD.

[23] Ídem.

[24] Ídem.

[25] Bernuy, J. (2008). Implementación de seguridad de la información mediante ISO-17799 plataforma BSD.

[26] Reyes. M. (2011). Propuestas para impulsar la seguridad informática en materia de educación

[27] Liao, J. (2022). The Three Key Layers of Any Cyber Defense System.

[28] IEC son las siglas en inglés para la Comisión Electrotécnica Internacional.

[29] Este sector comprende unidades económicas dedicadas principalmente a la transformación mecánica, física o química de materiales o sustancias con el fin de obtener productos nuevos; al ensamble en serie de partes y componentes fabricados; a la reconstrucción en serie de maquinaria y equipo industrial, comercial, de oficina y otros; y al acabado de productos manufacturados mediante el teñido, tratamiento calorífico, enchapado y procesos similares. Asimismo, se incluye aquí la mezcla de productos para obtener otros diferentes, como aceites, lubricantes, resinas plásticas y fertilizantes. El trabajo de transformación se puede realizar en sitios como plantas, fábricas, talleres, maquiladoras u hogares. Por lo general, estas unidades económicas usan máquinas accionadas por energía y equipo manual. INEGI. Economía y Sectores Productivos. (s.f).

[30] Statista. (2023). Participación porcentual del sector manufacturero en el producto interno bruto (PIB) en México de 2007 a 2022.

[31] Kaspersky. (2022). ICS cyberthreats in 2023 – what to expect.