Guía de implementación de medidas de ciberseguridad para empresas

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: Nomannoor943/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 de Normalización y Certificación (ANCE)

Bundesverband Mittelständische Wirtschaft
Asociación Alemana de la Pequeña y Mediana Empresa

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 cuarto y último volumen que versa sobre la importancia de la ciberseguridad en las empresas, así como acerca 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

// En una economía global caracterizada por el avance de la digitalización y la creciente aplicación de soluciones de la Industria 4.0 en las cadenas globales de valor, los sistemas administrativos y de producción de empresas se encuentran cada vez más interconectados. Si bien este intercambio continuo de datos ha incrementado significativamente la eficiencia de los procesos operativos, también ha implicado mayores riesgos en materia de ciberseguridad.

En América Latina, México ocupa el tercer lugar en ciberataques con 1.7 millones de intentos tan sólo en 2021. Según el estudio realizado por Deloitte (en 2020), el 62% de las empresas en México han sufrido ciberataques desde el inicio de la pandemia y al menos el 76% de estas han sufrido uno o dos ataques significativos al año.

Por esto mismo, diversas empresas internacionales han manifestado su preocupación sobre las condiciones de ciberseguridad a lo largo de sus cadenas de valor en el país. Uno de los motivos que encontraban era la escasa aplicación de estándares armonizados internacionalmente en la materia –como ISO/IEC 27001 e IEC 62443– por parte de sus proveedores. Con base en datos recientes, el 60% de los ciberataques se han originado en entidades que forman parte de la cadena de suministro. El punto principal de entrada han sido empresas pequeñas, donde se producen 92% de los incidentes de ciberseguridad que se experimentan a lo largo de las cadenas globales de valor.

La falta de estrategias integrales de ciberseguridad, incluyendo tanto elementos técnicos como de concientización, puede llegar a comprometer gravemente la economía de una empresa y sus clientes, ya sea de manera directa (por secuestro de información y extorsión) o indirecta (mediante efectos de reputación). Aquí, las pequeñas y medianas empresas (PyMEs) se encuentran en una situación muy difícil, ya que no todas cuentan con los medios para buscar una certificación en estándares internacionales o con personal especializado en materia de ciberseguridad.

En este sentido, este documento es parte de una serie de insumos que busca brindar recomendaciones para las PyMEs para que puedan mejorar su protección ante los riesgos crecientes en materia de ciberseguridad. Complementando las otras publicaciones de esta serie –sobre los riesgos de ciberseguridad que afectan a las empresas en México en la actualidad y el mapeo de los estándares nacionales e internacionales de ciberseguridad más importantes–, el presente espera ser una guía que permita poner en práctica políticas de ciberseguridad en las PyMEs en línea con los estándares globales. Por ello, integra recomendaciones para la implementación de una estrategia de ciberseguridad empresarial efectiva y accesible para las PyMEs, elaboradas por expertos y expertas de empresas internacionales y organismos de estandarización.

A partir de la definición de conceptos básicos asociados con la ciberseguridad, esta guía introduce y explica las herramientas de gestión de riesgos y las medidas de protección, y especifica a detalle cómo actuar ante incidentes de ciberseguridad para minimizar los daños. La estructura modular del documento permite hacer una lectura selectiva de las secciones individuales, acoplándose así a las necesidades particulares de las distintas empresas. Por ejemplo, el capítulo 5 presenta recomendaciones enfocadas a las aplicaciones específicas de los servicios de la nube, que son utilizados por un número cada vez mayor de empresas y, por lo tanto, merecen atención especial. Por su parte, el capítulo 6 aborda la ciberseguridad industrial y discute consideraciones particulares para salvaguardar la seguridad de las redes industriales dada su importancia económica en México.

2. Conceptos básicos de ciberseguridad

// En esta primera parte de la guía se asentarán las bases para comprender y aplicar las herramientas de ciberseguridad en un contexto empresarial. En particular, se discutirán las diferencias entre seguridad de la información y ciberseguridad, la identificación y clasificación de información personal y confidencial, así como importantes distinciones entre las tecnologías de la información (TI) y las tecnologías de operación (TO) en relación con la aplicación de medidas de ciberseguridad.

© Macrovector/Freepik

2.1 Seguridad de la información vs ciberseguridad

La seguridad de la información y la ciberseguridad son términos que a menudo se usan de manera indistinta, pero que en realidad tienen diferencias importantes. La seguridad de la información se refiere a la protección de la información contra el acceso, el uso, la divulgación, la interrupción, la destrucción o la modificación no autorizados de la misma. La ciberseguridad, por otro lado, se enfoca en la protección de los sistemas informáticos y la infraestructura conectada a internet contra ataques cibernéticos. Si bien los ataques cibernéticos pueden ser una forma común de comprometer la seguridad de la información, también existen riesgos físicos, como el robo de dispositivos de almacenamiento externos o el acceso no autorizado a documentos impresos. Tanto la seguridad de la información como la ciberseguridad son importantes para la protección de la empresa.

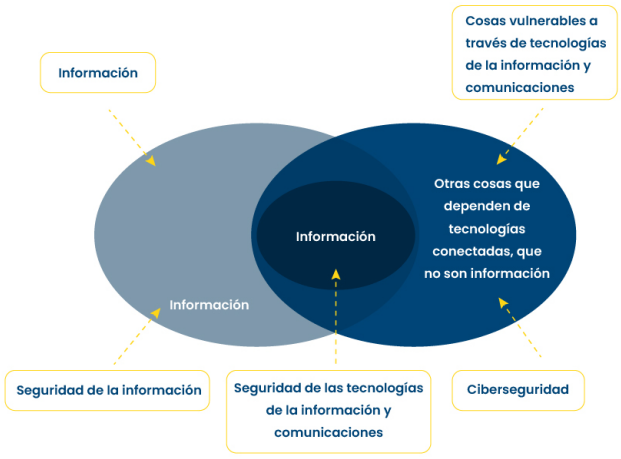


Gráfico 1. Ciberseguridad vs seguridad de la información. Elaborado por Pablo Corona, adaptación de .

2.2 Identificación y clasificación de información personal y confidencial

¿Qué información es importante proteger dentro de una empresa? Aquella que está compuesta por datos personales, datos personales sensibles y otros tipos de información confidencial que se especifican a continuación.

Las leyes de protección de datos personales en México definen que cualquier dato que puede contribuir a la identificación de una persona física es un dato personal. Algunos ejemplos serían: nombre y/o apellido, detalles de contacto (p. ej. dirección), nombres de usuario descriptivos, roles descriptivos (p. ej. alcalde de una ciudad) o la dirección de correo electrónico. Pero también incluyen datos como la dirección IP, el nombre de usuario en una aplicación, número de teléfono, datos de ubicación de una persona, así como características físicas, genéticas, mentales, económicas, culturales o sociales (como edad, tamaño, peso y sexo). Las empresas deben proteger los datos personales de sus clientes, proveedores y personal para evitar que terceros con acceso hagan mal uso de ellos; por ejemplo, mediante prácticas como el robo de identidad.

La Ley Federal de Protección de Datos Personales especifica los requisitos mínimos que toda entidad que trabaje con datos personales debe observar. Entre ellos debemos destacar los datos personales sensibles, cuyo mal uso o publicación no autorizada puede llevar a actos discriminatorios contra la persona o, incluso, poner en riesgo su seguridad. Ejemplos de datos personales sensibles son aquellos que versan sobre el estado de salud de una persona, su orientación sexual o su pertenencia a una religión o ideología. Estos datos requieren mayor grado de protección, ya que las consecuencias de un mal uso pueden ser muy graves.

La información confidencial engloba toda la información cuyo extravío puede representar un daño para la empresa, sus empleados o clientes. Los datos personales forman parte de esta categoría, que además abarca otra información de la empresa, como los borradores de contratos y comunicados internos o los estados financieros. Una buena manera de identificar el grado de confidencialidad de una pieza de información es preguntarse: ¿qué sucedería si esta información cae en las manos equivocadas? Si la respuesta es "nada", es muy probable que no se trate de información confidencial, como en el caso del menú semanal de la cantina. Sin embargo, en los casos mencionados arriba, la filtración de información puede implicar graves daños reputacionales y hasta poner en riesgo la seguridad de los individuos.

2.3 Confidencialidad, integridad y disponibilidad

Hay tres principios fundamentales para proteger la información y los sistemas de una organización de amenazas internas y externas, y estos son: confidencialidad, integridad y disponibilidad (CID). Juntos conforman la llamada "triada de la seguridad", en la cual se debe basar cualquier estrategia de ciberseguridad.
La confidencialidad se refiere a la protección de la información para que sólo sea accesible por personas autorizadas. Esta se logra mediante la implementación de controles de acceso, como contraseñas, autenticación de dos factores y la gestión de permisos.

La integridad se refiere a la exactitud y la consistencia de la información. Esto significa que la información no debe ser modificada de manera no autorizada. Se puede lograr mediante la implementación de controles de seguridad de datos, como firmas digitales y cifrado de datos.
La disponibilidad se refiere a la capacidad de acceder a la información y los sistemas cuando se necesitan. Esta se logra mediante la implementación de medidas de seguridad, como copias de seguridad y redundancia de sistemas.

La confidencialidad, la integridad y la disponibilidad trabajan juntas para proporcionar un enfoque integral de la seguridad. Si uno de estos pilares falla, los otros dos también pueden verse comprometidos. Por ejemplo, si

un atacante obtiene acceso no autorizado a información confidencial, la confidencialidad se ve comprometida. Si ese atacante modifica la información de manera no autorizada, la integridad también se verá afectada. Finalmente, si los sistemas se vuelven inaccesibles debido a un ataque cibernético, habrá fallas en la disponibilidad.

2.4 Diferencias entre tecnologías de la información (TI) y tecnologías de operación (TO) y su convergencia

La tecnología de la información (TI) se caracteriza por la aplicación de equipos de telecomunicación para tratar datos. Los sistemas de TI corporativos se ocupan de los sistemas y el software de "negocio", como es ERP, las bases de datos de los clientes y los programas de contaduría, entre otros. En cambio, la tecnología de las operaciones (TO) está enfocada en detectar y cambiar los procesos físicos a través de la monitorización y el control de dispositivos físicos. Abarca 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.

Aunque ambas tecnologías pueden trabajar en conjunto para potenciar sus funcionalidades, debemos comprender que sus utilidades son muy distintas y que los entornos en los que deben conservarse también difieren. Conocer las diferencias entre TI y TO es importante para garantizar una convergencia responsable y funcional en aplicaciones de la Industria 4.0.

Distintas prioridades en materia de ciberseguridad

Los sistemas de TI dan prioridad a la **confidencialidad** de los datos por encima de los otros elementos de la triada de ciberseguridad. Por ejemplo, si durante un tiempo no se puede acceder a los estados financieros mediante el software que utiliza la empresa (disponibilidad), esto puede causar un daño, pero el daño probablemente será mucho mayor si estos se publican (confidencialidad). En contraste, los sistemas de TO y de control industrial ponen por delante la **disponibilidad** de su tecnología, dado que una limitación de la misma, por ejemplo, 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.

Gráfico 2. 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)

El gráfico nos permite visualizar la inversión de las prioridades en materia de seguridad según se trata del área de sistemas de TO o TI.

Frecuencia de actualización

Existe un abismo entre el tiempo que se tarda en actualizar un sistema de TI y uno de TO. La tecnología TI es más vulnerable y por ello necesita actualizaciones constantes. Al tratarse de entornos más dinámicos, es fácil encontrar estos errores y solventarlos. Sin embargo, los sistemas de TO deben permanecer en marcha durante largos periodos de tiempo, por lo que no pueden ser parcheados a menudo, puesto que esto requeriría de un reinicio. Por desgracia, esto causa que a menudo se utilicen sistemas obsoletos de TO.

En los siguientes apartados nos enfocaremos en los sistemas de TI, ya que hoy en día estos son fundamentales para las operaciones de la gran mayoría de las empresas, independientemente de su sector. Los sistemas de TO se revisarán en el capítulo 7 de ciberseguridad industrial.

3. Gestión de riesgos de ciberseguridad

La gestión de riesgos es un proceso fundamental para implementar de forma adecuada un esquema de ciberseguridad que permita a las empresas identificar, evaluar y priorizar los riesgos para así reducir, controlar y mitigar su impacto en la confidencialidad, integridad y disponibilidad de la información y los servicios que soportan al negocio. No existe un solo control que elimine todos los riesgos, ni una estrategia de seguridad perfecta. Por ello, es vital que las organizaciones realicen y mantengan actualizado el proceso para la gestión de riesgos.

Cabe mencionar que el objetivo final de la gestión de riesgos es conocer cuáles son los controles y las acciones necesarias para atender estos riesgos, de manera que todas las actividades en este proceso puedan estar enfocadas en identificar el tipo de controles requeridos, dónde son necesarios y qué tantos recursos se dedicarán a diseñarlos, implementarlos y mantenerlos.

Identificación de riesgos

Cada empresa es diferente, opera en sectores distintos, y hay diversos tamaños y modelos de negocio; por esto, es fundamental iniciar con un mapeo riguroso de los riesgos en materia de ciberseguridad a los cuales se enfrenta la empresa. Una buena forma de comenzar identificando estos riesgos es preguntarse cuál es la información o cuáles son los procesos que resultan fundamentales para el funcionamiento del negocio: puede ser una plataforma de pedidos, datos de clientes, listas de precios, contratos no publicados, secretos industriales, sistemas de cotización u otra información o sistema sensible. Estas "joyas de la corona" serán los elementos que tienen mayor probabilidad de estar en la mira de los ciberdelincuentes para realizar, por ejemplo, un secuestro de información o un ataque al sistema que les permita extorsionar.

Una vez que se han identificado estos elementos clave del negocio, se puede continuar con

© Pressfoto/Freepik

los riesgos que presenta cada uno. Esta es una labor que no corresponde solamente a las áreas de tecnología o de sistemas. Identificar los riesgos potenciales requiere de una comprensión completa del entorno interno y externo. Por ello, las empresas deben llevar a cabo un análisis FODA (Fortalezas, Debilidades, Oportunidades, Amenazas) con regularidad para detectar cualquier cambio que pueda suponer un riesgo.

Existen varias técnicas que pueden ayudar a complementar esta identificación, como las evaluaciones de vulnerabilidad y las pruebas de penetración, dos técnicas diferentes utilizadas por los equipos de seguridad de TI para identificar riesgos de seguridad en las redes. Ambas forman parte de regulaciones y estándares internacionales en materia de ciberseguridad, como PCI, HIPAA, FISMA e ISO/IEC 27001. Son herramientas que se complementan para lograr una comprensión integral de las vulnerabilidades presentes en un ecosistema de TI.

El análisis de vulnerabilidad automatizado genera un informe que abarca todos los riesgos de seguridad encontrados en el sistema y establece niveles de priorización. Entre las vulnerabilidades más comunes, o puertas traseras abiertas que le pueden dar acceso a cibercriminales a manipular información o sistemas clave, se encuentran:

- Contraseñas almacenadas en archivos accesibles.
- Permisos excesivos de los usuarios de la red.
- Datos no encriptados.
- Software sin parches.
- Herramientas de ciberseguridad mal configuradas.
- Dispositivos mal configurados.

En contraste, las pruebas de penetración son simulaciones de un ataque real a la infraestructura de TI por "hackers éticos" que intentan romper las defensas del ecosistema, adaptando el ataque en respuesta a las resistencias. Antes de conducir pruebas de penetración, se requiere una especificación clara de qué aspectos y segmentos del ecosistema de TI se buscan evaluar.

Las principales diferencias entre ambas herramientas pueden observarse en la tabla 1.

Considerando el costo de las pruebas de penetración, en el caso de las PyMEs se recomienda hacerlas enfocadas en la identificación de vulnerabilidades en los sistemas que contienen la información más crítica de la empresa, que es la que tiene mayor probabilidad de ser atacada. No obstante, a pesar de su costo, es aconsejable usar esta herramienta en la medida de lo posible, ya que puede generar grandes aprendizajes para el diseño de planes de respuesta ante incidentes reales y evitar daños significativos gracias a la experiencia recabada en el simulacro.

Categorización de riesgos

Los riesgos identificados en el análisis FODA, los análisis de vulnerabilidad y las pruebas de penetración deben clasificarse en diferentes categorías como operacionales, financieros, estratégicos y de cumplimiento, entre otros, para que puedan ser gestionados de manera efectiva. Los riesgos de ciberseguridad pueden

	Análisis de vulnerabilidad	Pruebas de penetración
Alcance	Amplia – busca detectar el mayor número de riesgos	Focalizada – busca identificar riesgos específicos a profundidad
Ejecución	Automatizado, como parte del software	Componentes automatizados y manuales, requiere profesionales de TI o "hackers éticos"
Intervalos	Mínimo una vez cada cuatro meses	1 o 2 veces al año
Duración	20 minutos a 4 horas	1 a 3 semanas
Costo	Bajo	Alto
Fortalezas	• Da una lista completa de los riesgos potenciales de seguridad • Sugiere acciones para remediar los defectos	• Da información específica sobre cómo pudiera suceder un ataque • Pone a prueba la reacción del ecosistema ante un ataque
Debilidades	• No puede detectar riesgos de seguridad desconocidos	• No proporciona información completa sobre los riesgos

Tabla 1 Diferencias entre análisis de vulnerabilidad y pruebas de penetración. Elaboración propia.

ser de diferentes tipos, como malware, phishing, ataques de fuerza bruta, etc. Cada uno de estos debe ser identificado y categorizado adecuadamente.

Evaluación y priorización de riesgos de ciberseguridad

Para poder elegir medidas de protección adecuadas para los riesgos identificados, se debe evaluar para cada riesgo de ciberseguridad: 1) su probabilidad de ocurrencia y 2) su impacto potencial para entender su posible repercusión. Con base en esto será necesario priorizar los riesgos, enfocándose en aquellos que tienen más probabilidad de causar el mayor daño a la empresa. Ante la limitación de recursos en el contexto de las PyMEs frente a las grandes empresas, resulta fundamental crear una lista sólida de riesgos prioritarios y enfocar los recursos en estos.

Estrategias de mitigación de riesgos de ciberseguridad

Ante los riesgos de ciberseguridad de alta prioridad, las organizaciones deben tener planes de tratamiento de riesgos que implican contar con recursos, acciones y respuestas planificadas para manejar el riesgo en caso de llegar a materializarse. Esto incluye tener planes de contingencia y continuidad de operaciones para limitar el daño lo más posible en caso de un ciberataque. Así, la empresa podrá responder de manera planificada si llegara a presentarse una falla de seguridad, otorgándole a la vez un mayor margen de recuperación. Además, este tipo de acciones suelen mejorar la imagen corporativa, con lo cual se reducen posibles pérdidas financieras y de confianza. Para conocer más sobre cómo podemos prepararnos para un ciberataque a nuestras "joyas de la corona" y definir los planes de acción haz clic aquí.

Para complementar estos planes de tratamiento de riesgos, también se deben implementar medidas de seguridad apropiadas, como firewalls, sistemas de detección de intrusiones, cifrado, autenticación de dos factores, entre otras, y así reducir la exposición al riesgo. Puedes encontrar más detalles sobre estas medidas en el capítulo 5 de esta guía. Sin embargo, cabe resaltar que aún si se cuenta con las mejores medidas de ciberseguridad, estas no eliminan la necesidad de tener planes de tratamiento de riesgos para nuestros activos más importantes, ya que ningún sistema de protección es perfecto y cada día se desarrollan nuevas ciberamenazas.

Monitoreo y revisión de riesgos de ciberseguridad

Los riesgos de ciberseguridad pueden cambiar rápidamente. Debido a la velocidad con la que va creciendo la diversidad de ciberamenazas, es crucial revisar y actualizar con regularidad la estrategia de gestión de riesgos de ciberseguridad. Por ello, se recomienda realizar evaluaciones periódicas de la gestión de riesgos en materia de ciberseguridad al menos una vez cada cuatro meses, para asegurarse de que se están tomando las medidas adecuadas y de que se están alcanzando los objetivos previstos.

También se recomienda complementar estas evaluaciones internas con auditorías externas de ciberseguridad y seguridad de la información, aunque sea a intervalos de tiempo más largos. Estas pueden proporcionar una segunda mirada para identificar vulnerabilidades y riesgos y sugerir posibles soluciones. Para beneficio de las empresas, muchas de las organizaciones que efectúan este tipo de auditorías emiten sellos o distintivos de confianza luego de comprobar que la empresa cumple con las pautas necesarias en materia de calidad y seguridad. Si bien tales distintivos no son obligatorios, ayudan a que las organizaciones transmitan más confianza y credibilidad al usuario en temas relacionados con seguridad, atención al cliente, protección de datos y protección de pagos, entre otros.

Cultura de gestión de riesgos de ciberseguridad

Cualquier estrategia de gestión de riesgos de ciberseguridad tiene que estar anclada en la cultura organizacional, fomentando que cada empleado comprenda la importancia de este proceso y participe activamente en él.

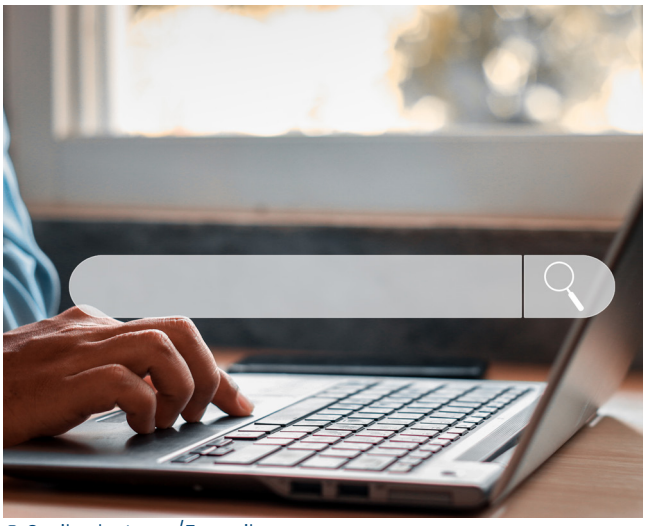
En la mayoría de los casos, son las fallas humanas y no las tecnológicas las que permiten la entrada de cibercriminales en los sistemas.

Para fomentar esta cultura en torno a la ciberseguridad, es vital contar con medidas de capacitación y desarrollo continuas que concienticen a las y los empleados sobre la importancia de la ciberseguridad y el creciente riesgo que representan las ciberamenazas para las empresas, así como las mejores prácticas de ciberseguridad y cómo cada persona puede contribuir a mitigar los riesgos en su trabajo diario.

En el siguiente capítulo se discutirán elementos importantes como la identificación de información personal y confidencial, guías para una navegación segura y la capacitación sobre los peligros de la ingeniería social y el phishing, mismos que deben formar parte de estas capacitaciones para todo el personal.

4. Concientización básica de seguridad

La concientización básica de seguridad se ha convertido en un factor crucial para prevenir ciberataques en empresas desarrolladoras de aplicaciones en línea, así como en los usuarios que hacen uso de ellas. Ambos terminan siendo dos caras de una misma moneda, ya que al ser conscientes de las buenas prácticas de seguridad, la identificación y clasificación de información personal y confidencial, así como la prevención de ingeniería social y el manejo responsable de las redes sociales, se pueden fortalecer las defensas cibernéticas y evitar incidentes desastrosos. En la presente sección veremos cómo estas medidas ayudan a prevenir ataques.



© Smilephotoap/Freepik

4.1 Identificación y clasificación de información personal y confidencial

Es fundamental que todo el personal reciba capacitación acerca de cómo identificar la información personal y confidencial, tal como se describe en el capítulo 2, además de cómo tratarla para evitar su exposición. Primero que nada, debemos ser conscientes de qué información compartimos y utilizamos en los servicios en línea. Muchos de los servicios que parecieran ser gratuitos en realidad lo que buscan no es dinero sino nuestra aprobación para el uso de nuestros datos personales, esto principalmente con fines comerciales y de perfilamiento para generar publicidad dirigida a los gustos, intereses y relaciones de cada usuario. Los datos como nombre, número de identificación o datos de ubicación, identidad física, fisiológica, genética, mental, económica, cultural o social de la persona, pueden ser utilizados para perfilarla y con ello obtener información que pueda ser utilizada para fines no alineados con sus intereses.

De la misma manera, las organizaciones que recaban datos personales y las personas que los procesan dentro de las mismas deben asegurarse de sólo tratar dicha información para los fines para los cuales el titular de los datos dio su consentimiento. Para esto deben tenerse en cuenta los requisitos de privacidad de datos:

i. En el diseño y funcionalidades de nuestros productos y soluciones.
ii. Mientras se prestan los servicios (p. ej. cuando se alojan soluciones del cliente que contienen datos personales o cuando se accede de forma remota a los sistemas del cliente).

Proteger los datos desde el diseño implica considerar los problemas de privacidad y protección de datos desde el comienzo del desarrollo del producto o la ingeniería de la solución. Eso significa que en la fase de diseño de cualquier actividad de recopilación y procesamiento (que involucre datos personales) y en el momento del procesamiento en sí, se deben tomar en cuenta las medidas técnicas y/u organizativas apropiadas.

También la información confidencial de la organización debe ser clasificada y protegida adecuadamente, por lo que deben establecerse reglas para indicar qué medios se pueden utilizar para el almacenamiento, transmisión

y procesamiento de la información y los datos personales. Por ejemplo, señalar si está permitido el uso de correos electrónicos o medios de almacenamiento removible o de nube en el entorno organizacional.

Navegación segura

Es importante capacitar a todo el personal sobre la navegación en la red para que tomen las siguientes precauciones:

- Comunicarse a través de conexiones seguras.
- Mantener actualizado el navegador de todos los dispositivos.
- Verificar que el sitio que se visita está correctamente escrito y no tiene cambios o caracteres faltantes, extra o similares.
- Navegar únicamente en sitios seguros que utilizan el protocolo HTTPS.
- Descargar sólo archivos o documentos de páginas web confiables.
- Utilizar contraseñas seguras para todas las cuentas y cambiarlas periódicamente.
- No usar la misma contraseña para más de una cuenta.
- Ser extremadamente cauteloso en caso de recibir correos sospechosos, en especial si no se conoce al remitente.

En las siguientes imágenes se puede apreciar la alta calidad que hoy en día tienen las páginas web falsas y, sin embargo, mediante una revisión crítica de la dirección del sitio podemos aprender a discernir entre las páginas confiables y aquellas que no lo son.

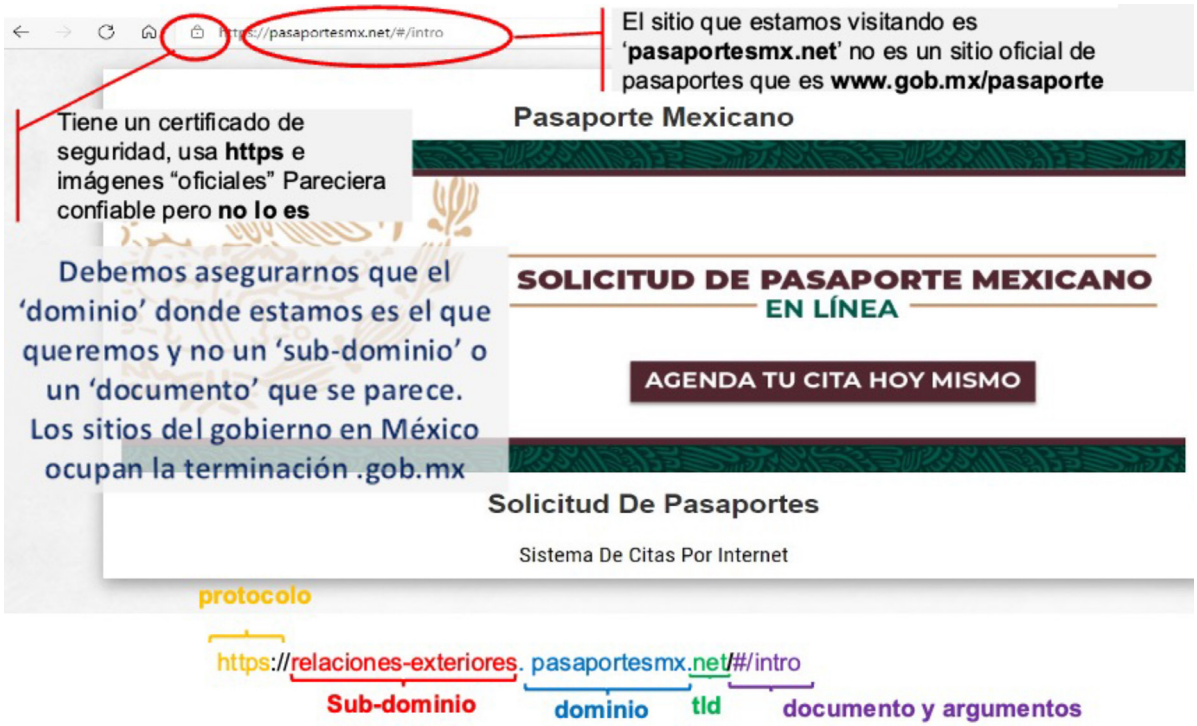


Gráfico 3. Identificar una dirección web segura, imagen 1/2. Elaborado por Pablo Corona.

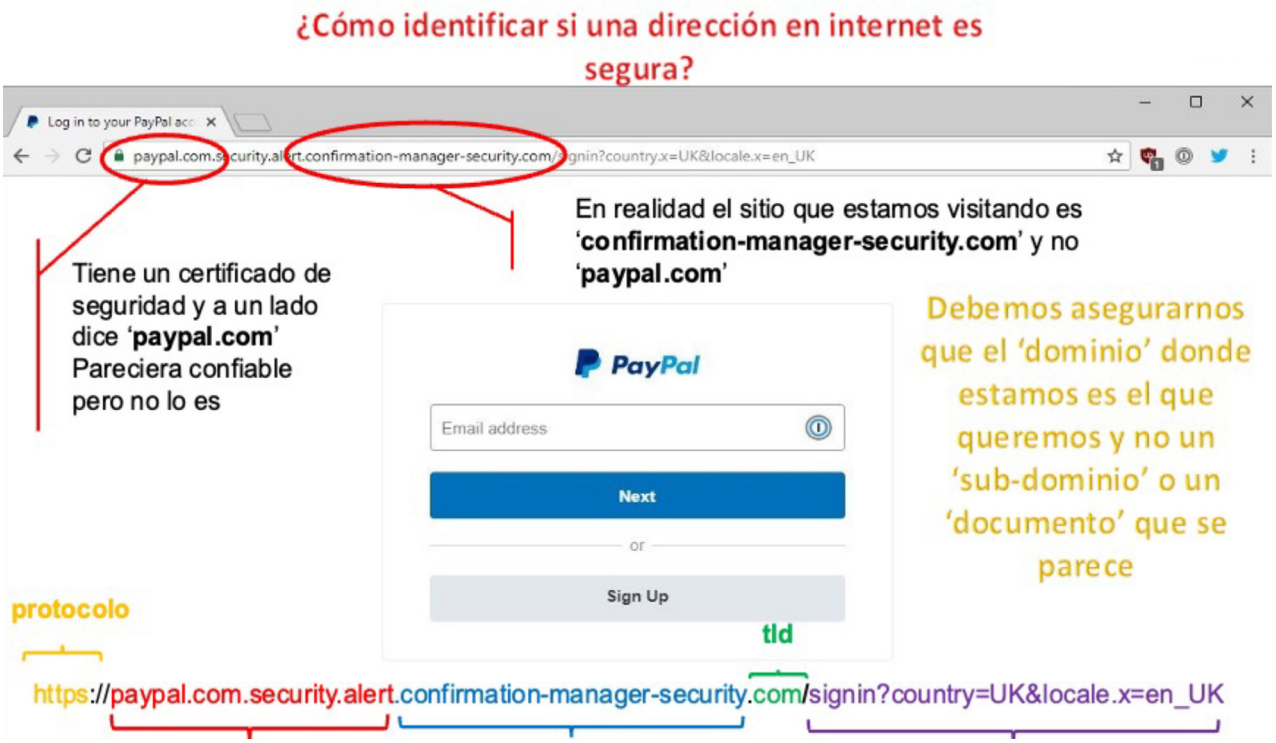


Gráfico 4. Identificar una dirección web segura, imagen 2/2. Elaborado por Pablo Corona.

4.2 Ingeniería social y redes sociales

Protección de datos personales y de la empresa en redes sociales

Las redes sociales en el sector empresarial han adquirido una importancia cada vez mayor en los últimos años, creando nuevas oportunidades de negocio y para participar en las conversaciones globales. Sin embargo, esta nueva tecnología también trae consigo nuevos riesgos. Definir algunas reglas básicas de participación dentro de las redes sociales nos ayudará a comunicarnos de forma segura.

Particularmente, existe el peligro de que la frontera entre la vida profesional y la vida privada se desdibuje. Los datos personales se mezclan con información relacionada con las empresas y los hechos a menudo se enriquecen con opiniones privadas. Los principales riesgos son la divulgación de información privada corporativa y la violación de los derechos de autor y de propiedad intelectual.

El escándalo que presentamos en el Caso 1 sobre una red social y una empresa de consultoría política nos da una buena idea de los riesgos en los que podemos incurrir tanto como usuarios de redes sociales, como siendo una plataforma de redes sociales, si nos descuidamos al proteger nuestra información o la de nuestros usuarios.

Caso 1. Empresa de consultoría política (2018)

En 2018 se reveló el escándalo de una empresa de consultoría política que obtuvo acceso indebido a datos personales de millones de usuarios a través de una aplicación en una de las redes sociales más importantes del mundo.

La aplicación se presentaba como una prueba de personalidad y, al obtener el consentimiento de los usuarios para acceder a sus datos, recopilaba información de su red de amigos en la plataforma. Esto permitió que la empresa obtuviera datos de manera masiva, incluyendo información personal, preferencias políticas y patrones de comportamiento de los usuarios.

La principal problemática radicó en que la empresa utilizó estos datos para elaborar perfiles psicológicos y realizar análisis de comportamiento con fines políticos. Además, se alega que usó estos perfiles para influir en la opinión pública y la toma de decisiones políticas durante las elecciones presidenciales de Estados Unidos en 2016, así como en otros procesos electorales alrededor del mundo.

El caso generó una gran indignación y preocupación sobre la privacidad y la seguridad de los datos en las redes sociales. Se puso en evidencia la falta de control y supervisión por parte de la red social en cuanto al acceso y uso de datos por parte de terceros, así como la falta de conciencia por parte de los usuarios sobre cómo sus datos personales podían ser utilizados sin su conocimiento.
Este caso tuvo un impacto significativo tanto para la empresa de consultoría política, como para la red social. Esta última enfrentó una fuerte crítica por su falta de protección de datos y su manejo inadecuado de la privacidad de los usuarios, y experimentó una pérdida de confianza por parte de los usuarios y una disminución en su valor de mercado.

A partir de esto y de las medidas que implementó la red social tras el escándalo se puede apreciar cómo tanto desde la perspectiva del usuario, como desde la perspectiva de la plataforma podemos implementar mecanismos para proteger la información personal.

Como plataforma, se puede restringir el acceso a la API (Interfaz de Programación de Aplicaciones) de la plataforma para reducir la cantidad de datos personales que los desarrolladores de aplicaciones pueden obtener, medida que la red social implementó tras el incidente. Otras medidas incluyeron mejorar la transparencia de los procesos de consentimiento de los usuarios y de su control de privacidad en las configuraciones personales. Finalmente, se instauraron auditorías periódicas de los desarrolladores de aplicaciones para garantizar que estos cumplan con las políticas de privacidad y seguridad de la empresa, y eliminar recopilaciones de datos no autorizadas.

Desde la perspectiva de los usuarios, este caso muestra la importancia de revisar cada cierto tiempo las aplicaciones y servicios que están conectados a la cuenta de la red social y revocar los permisos de acceso de aplicaciones no utilizadas o sospechosas, así como limitar el acceso sólo a las aplicaciones confiables. En este contexto, resulta importante estar atento a la configuración predeterminada de privacidad, revisar periódicamente las opciones de privacidad y ajustarlas según las preferencias personales, ya que las redes sociales actualizan sus políticas y configuraciones de privacidad con regularidad.

Ingeniería social

Por otro lado, existen los ataques de ingeniería social. La ingeniería social se refiere a distintas técnicas de manipulación que usan los ciberdelincuentes para obtener información confidencial de individuos o empresas. Los ciberdelincuentes engañan a sus víctimas pretendiendo ser personas de soporte técnico, compañeros de trabajo o incluso superiores. De esta forma, buscan encontrar acceso a información confidencial, como contraseñas, o suplantar la identidad de la persona para, por ejemplo, autorizar pagos y así extraviar recursos. Los ciberdelincuentes pueden diseñar estas prácticas fraudulentas para que sean más creíbles a partir de la información que puedan obtener sobre la persona y la empresa, por ejemplo, en sus redes sociales.

Una de las técnicas más recurrentes de ingeniería social es el phishing, que busca robar credenciales e información de usuarios al hacerse pasar por páginas y empresas con las que el usuario suele tener contacto, solicitándole que acceda a un sitio falso para robar sus datos de acceso o buscando que instale o ejecute un archivo adjunto que contiene software malicioso.

En el siguiente gráfico podemos observar algunas recomendaciones para evitar el *phishing*.

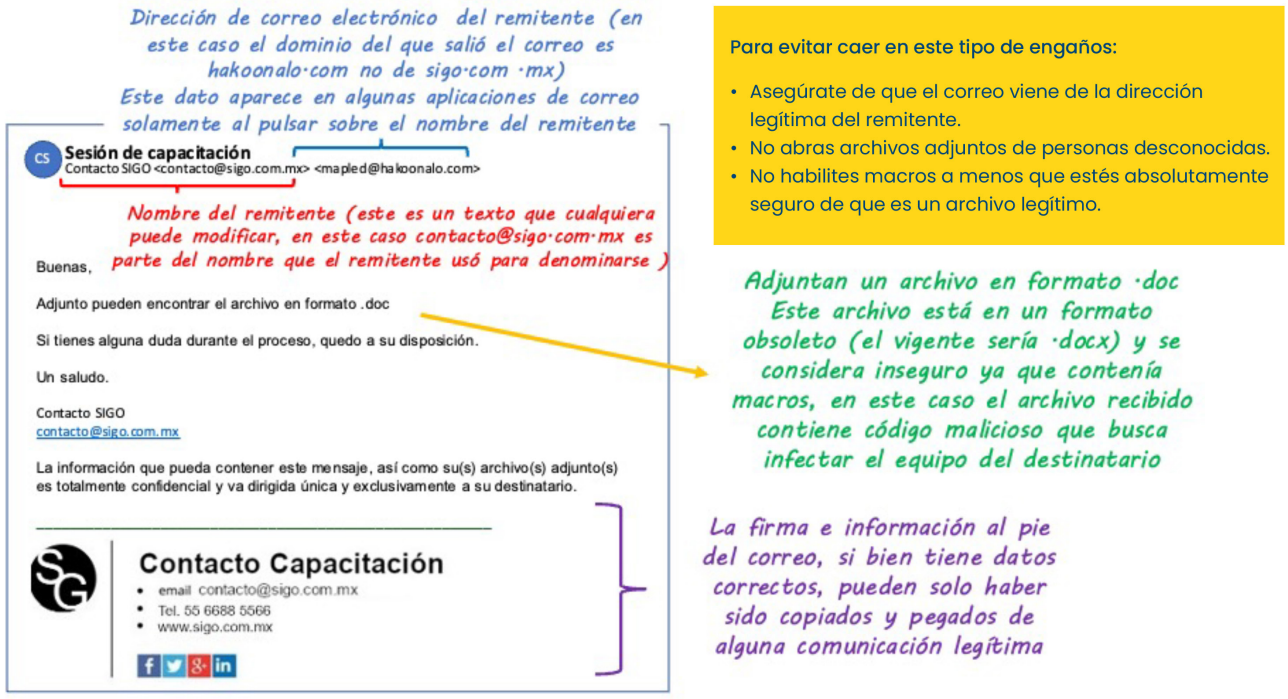


Gráfico 5. *Phishing*. Elaborado por Pablo Corona.

Como se puede apreciar en la imagen, hoy en día el phishing se practica de manera bastante sofisticada, haciendo difícil la distinción a primera vista entre correos y mensajes falsos y aquellos que son fidedignos.

Sin embargo, podemos proteger a nuestra empresa y nuestros datos si tenemos cuidado con las solicitudes y mensajes sospechosos: nunca hagas clic en enlaces sospechosos, ni proporciones información personal a través de mensajes no confiables, y ten precaución al aceptar solicitudes de amistad o interactuar con perfiles desconocidos. El "Manual Básico de Ciberseguridad para la Micro, Pequeña y Mediana Empresa" de la Guardia Nacional (2023), nos brinda lineamientos específicos para la protección contra el *phishing* mediante correos electrónicos, misma que puedes consultar aquí.

A nivel organizacional es fundamental garantizar que todo el personal reciba capacitación sobre el *phishing* y los ataques de ingeniería social, de manera que estén informados sobre las tácticas utilizadas por los atacantes para obtener información confidencial. Estas capacitaciones deben mostrar cómo aprender a identificar correos electrónicos o mensajes falsos que intentan engañar para obtener información personal o credenciales de inicio de sesión. Del mismo modo, los tests (como los señalados en el Caso 1) son una herramienta común para obtener información de los usuarios y posteriormente aplicar estrategias de ingeniería social. Se puede encontrar aquí una guía a detalle sobre los riesgos de la ingeniería social, el *phishing* y otras tácticas fraudulentas, y cómo usar esta información para formar al personal.

Contar con una capacitación periódica sobre los riesgos es un elemento fundamental de cualquier estrategia de ciberseguridad, ya que la mayoría de los ciberataques exitosos no se deben a fallas técnicas, sino a fallas humanas. El caso del ciberataque a una compañía productora cinematográfica (2014) evidencia la importancia de proteger nuestras empresas contra este tipo de prácticas, así como las consecuencias que pueden resultar al no hacerlo.

Caso 2. Productora cinematográfica (2014)

En noviembre de 2014 atacantes infiltraron la red de uno de los conglomerados de medios de comunicación más importantes de EE. UU. y obtuvieron acceso a una gran cantidad de información confidencial y sensible. El grupo de hackers autodenominado „Guardians of Peace" (Guardianes de la Paz) se atribuyó la responsabilidad del ataque.

Los atacantes lograron infiltrarse en la red de la empresa mediante técnicas de ingeniería social, *phishing* y explotación de vulnerabilidades en el software. Una vez dentro de la red, llevaron a cabo una serie de actividades maliciosas, como el robo y filtración de información confidencial, la destrucción de datos y el bloqueo de los sistemas informáticos.

Como resultado del ciberataque se filtraron numerosos documentos internos de la compañía, como correos electrónicos, contratos, guiones de películas y datos personales de empleados y artistas. La filtración de esta información generó consecuencias significativas para la compañía, incluyendo daños a su reputación, pérdida financiera y posibles repercusiones legales. El incidente destacó la importancia de concientizar en las empresas sobre las prácticas fraudulentas como el *phishing* y la ingeniería social para mantener protegida la información sensible.

5. Herramientas de protección

Como respuesta a la identificación y priorización de riesgos tenemos el *hardening* o robustecimiento de un ecosistema de TI, que se refiere al conjunto de acciones que apuntan hacia una reducción de la superficie de ataque. La superficie de ataque se compone de todas las entradas, defectos o puertas traseras en un sistema que pueden servir como rutas potenciales de un ciberataque. 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.

Ejemplos importantes de acciones de *hardening* incluyen los siguientes apartados.

© Rawpixel.com/Freepik

5.1 Controles de acceso

Los controles de acceso son los guardias de nuestros sistemas de TI y sirven para filtrar quién sí tiene permiso para acceder y quién no. En este sentido, la autenticación y la autorización como elementos del control de acceso son herramientas esenciales para garantizar la seguridad y la protección de la información y de los sistemas de las empresas.

Gráfico 6. Autenticar y autorizar. Elaborado por Pablo Corona, adaptación de Microsoft Zero Trust Architecture.

5.1.1 Autenticación

La autenticación es el proceso de verificar la identidad de un usuario que intenta acceder a un sistema o aplicación; se utiliza para garantizar que sólo los usuarios autorizados tengan acceso. La autenticación se logra mediante el uso de credenciales de autenticación, como nombres de usuario y contraseñas, o mediante el uso de tecnologías de autenticación más avanzadas, como el escaneo de huellas dactilares o la autenticación de dos factores. Existen diferentes tipos de autenticación que pueden ser utilizados para garantizar la seguridad de los sistemas y la información. Uno de los más comunes son las contraseñas, donde se requiere que los usuarios ingresen un nombre de usuario y una contraseña para verificar su identidad.

Contraseñas

Las contraseñas son una herramienta de protección clave. Sin embargo, a menudo son la única línea de defensa para proteger la información, por lo que es importante asegurarse de que sean lo suficientemente fuertes y se manejen de forma adecuada.

Las empresas pueden implementar políticas de contraseñas para garantizar que los empleados usen contraseñas seguras y que las cambien con frecuencia. Estas también pueden incluir, por ejemplo, restricciones sobre la reutilización de contraseñas antiguas o el uso de contraseñas fáciles de adivinar, obligando a utilizar otras que sean más seguras y complejas.

Autenticación de dos pasos

El segundo factor de autenticación es una medida cada vez más común para complementar las contraseñas como mecanismos de autenticación. En la mayoría de los casos, el segundo factor se refiere a algo que el usuario tiene en su poder, como un teléfono celular o una tableta. Se aplica a través de una aplicación móvil de autenticación, que se sincroniza con la cuenta en línea del usuario y genera un código de seguridad único que cambia cada pocos segundos. Para acceder a la cuenta, el usuario debe ingresar este código en la página de inicio de sesión junto con su contraseña. A pesar de que puede ser un poco más molesto para el usuario, es una medida de seguridad necesaria para proteger la información crítica.

Existen aplicaciones como Google Authenticator, Microsoft Authenticator y algunos gestores de contraseñas que generan estos códigos de un solo uso para ser sincronizados con cada una de nuestras aplicaciones, servicios de correo, mensajería, sitios web y aplicaciones corporativas. Sin embargo, la autenticación por sí sola no es suficiente para controlar el acceso a la información; debe combinarse con la autorización para garantizar que únicamente los usuarios autorizados tengan acceso a los sistemas.

5.1.2 Autorización

Es el proceso de otorgar acceso a recursos específicos después de que un usuario ha sido autenticado. Se utiliza para garantizar que los usuarios tengan acceso sólo a los recursos que necesitan para realizar su trabajo y evita que los usuarios no autorizados accedan a información confidencial.

La autorización se puede implementar mediante diferentes mecanismos de control de acceso. Uno de los métodos más comunes es el control de acceso basado en roles (RBAC, por sus siglas en inglés), que asigna permisos y privilegios en función del rol del usuario en la organización. Por ejemplo, un administrador de sistemas puede tener permisos para acceder y configurar los sistemas, mientras que un empleado de contabilidad sólo tendrá acceso a los datos financieros de la empresa. Otro método de autorización es el control de acceso basado en atributos (ABAC, por sus siglas en inglés), que se basa en los atributos del usuario y de los recursos para determinar los permisos y privilegios de acceso. ABAC utiliza una política de control de acceso que define los criterios para otorgar o denegar el acceso a los recursos, como la hora del día, la ubicación geográfica o el nivel de seguridad requerido.

5.1.3 Bitácoras

Una de las herramientas más importantes en la defensa contra las amenazas cibernéticas y que ayuda complementar los mecanismos de autenticación y autorización son las bitácoras o logs, que registran la actividad de los usuarios y los eventos de los sistemas y fungen como las cámaras de vigilancia de nuestros sistemas de TI. La recopilación y análisis de las bitácoras permite a los administradores de seguridad detectar y responder a los incidentes de seguridad de manera oportuna y efectiva.

Las bitácoras son archivos que contienen información detallada sobre las acciones que se han realizado en los sistemas, como el inicio de sesión de los usuarios, las actividades efectuadas en los sistemas, los cambios de configuración o los accesos no autorizados. La implementación de una política de registro de eventos es una práctica recomendada para la mayoría de los sistemas informáticos, ya que permite identificar patrones de actividad y detectar actividades sospechosas.

El análisis de las bitácoras puede hacerse de diferentes formas, y el enfoque dependerá del tipo de amenaza que se esté monitoreando. Por ejemplo, el análisis de las bitácoras puede ayudar a identificar patrones de acceso inusual, como el inicio de sesión en un sistema a una hora no habitual o el acceso a un archivo de datos que no corresponde al perfil del usuario. Además, también puede ser útil para detectar actividades malintencionadas, como intentos de acceso no autorizado.

5.1.4 *Antimalware*

El *antimalware*, también conocido como software antivirus, es una herramienta esencial en el arsenal de seguridad de cualquier organización. Su principal función es detectar, prevenir y eliminar virus, troyanos, gusanos y otros tipos de *malware* que pueden infectar los sistemas informáticos. La importancia de contar con una solución *antimalware* radica en la creciente cantidad de amenazas que existen en línea, ya que los ciberdelincuentes desarrollan constantemente nuevos tipos de *malware* para comprometer la seguridad de los sistemas y robar información valiosa.

Es fundamental elegir una solución confiable y actualizada. Las soluciones *antimalware* deben ser capaces de detectar las últimas amenazas y proporcionar una protección en tiempo real. Otra práctica recomendada es programar análisis regulares del sistema para buscar *malware* oculto. Además, se requieren actualizaciones frecuentes del software *antimalware* para la detección de las amenazas más recientes.

Las soluciones *antimalware* modernas incluyen varios componentes para revisar los archivos ejecutables, los archivos de ofimática, las páginas web visitadas y los archivos adjuntos a correos electrónicos, así como validar los procesos que se cargan en la memoria y detectar comportamientos anómalos en la red y los sistemas de archivos. Algunos ejemplos de soluciones *antimalware* incluyen Norton Antivirus, McAfee Antivirus, Kaspersky Antivirus y Avast Antivirus.

5.1.5 Actualizaciones

Las actualizaciones de software son esenciales para mantener la seguridad de los dispositivos y protegerlos contra vulnerabilidades. A menudo incluyen parches de seguridad y correcciones de errores que solucionan vulnerabilidades que podrían ser explotadas por ciberdelincuentes, quienes suelen aprovechar el software desactualizado para lanzar ataques.

© Shahriarshanto888/Freepik

Existen varias prácticas recomendadas para implementar una política efectiva de actualizaciones de software. En primer lugar, es importante establecer un plan de actualización regular. Esto puede incluir la programación de actualizaciones automáticas en horarios no laborales para minimizar el impacto en la productividad. Otra práctica es mantener un registro de las actualizaciones; de esta manera, se puede realizar un seguimiento de qué sistemas han sido actualizados y cuándo. Algunos ejemplos del software que debe mantenerse actualizado son el sistema operativo, el software de seguridad, los navegadores web y las aplicaciones empresariales. En la mayoría de los casos, estos programas incluyen opciones de actualización automática para simplificar el proceso.

El caso del ciberataque a una empresa de informes crediticios ilustra la importancia de mantener nuestro software actualizado, en especial el *antimalware*, y nos da una idea de los costos que puede tener para una empresa el no hacerlo.

Caso 3. Ataque a empresa de informes crediticios (2017)

En 2017 tuvo lugar un incidente que impactó a una empresa especializada en evaluación crediticia. En dicho evento, delincuentes cibernéticos consiguieron ingresar a datos sensibles de alrededor de 147 millones de personas. Esta información englobaba nombres, números de identificación social, fechas de nacimiento y detalles de tarjetas de crédito.

El ataque se originó a través de una vulnerabilidad en el software de gestión de vulnerabilidades de la compañía que no había sido actualizado con el último parche de seguridad disponible. La brecha de seguridad habría sido evitable si la empresa hubiera aplicado las mejores prácticas de seguridad, como mantener el software actualizado, implementar controles de acceso robustos y contar con un programa integral de gestión de vulnerabilidades.

En este caso, los atacantes explotaron esta vulnerabilidad y lograron ingresar a los sistemas, obteniendo acceso a una gran cantidad de datos sensibles de los consumidores. Como consecuencia del ciberataque, la empresa experimentó un daño significativo a su reputación, afectando su imagen de marca, aunado a las fuertes implicaciones financieras, ya que enfrentó una serie de demandas legales y regulatorias, lo que resultó en costos legales y multas. Todo esto sin mencionar el impacto a las personas afectadas que pudieron haber incluido la posibilidad de robo de identidad, fraude financiero y daño a su historial crediticio; efectos que pueden tener repercusiones a largo plazo en su vida financiera y personal.

En el ya mencionado Manual Básico de Ciberseguridad para la Micro, Pequeña y Mediana Empresa, publicada por la Guardia Nacional (2023), se pueden encontrar políticas de seguridad en mecanismos de pagos electrónicos que indican cómo proteger específicamente la información financiera de los clientes y garantizar transacciones financieras seguras.

5.1.6 Respaldos

Los respaldos de la información son clave para proteger los datos de la empresa contra pérdidas accidentales o ataques de malware. Estos consisten en hacer una copia de seguridad de los archivos y documentos críticos almacenados en el dispositivo. La importancia de los respaldos radica en que, en caso de sufrir un incidente de seguridad, se puede recuperar la información perdida sin interrupciones significativas en las operaciones de la empresa.

Para implementar una política efectiva de respaldos de datos es necesario definir qué datos son críticos para la empresa y con qué frecuencia se deben realizar los respaldos. Por ejemplo, los datos financieros y los registros de clientes pueden ser críticos y requerir de un respaldo diario o semanal, mientras que otros datos pueden ser menos importantes y por ende efectuarse con menor frecuencia.

Además de hacer respaldos con regularidad es vital el almacenarlos en un lugar seguro y separado de los datos originales. De preferencia, se deben usar medios que siempre desconectados y que sólo se conecten para realizar los respaldos, que estén cifrados y que estén bien protegidos físicamente para evitar un acceso no autorizado. Para ello, existen varias herramientas disponibles que incluyen software de respaldo automático y servicios de almacenamiento en la nube. El uso de una combinación de herramientas de respaldo puede garantizar una mayor protección de los datos de la empresa.

Por último, es fundamental comprobar que los respaldos funcionen adecuadamente mediante pruebas regulares de recuperación de datos, evaluando el tiempo del proceso de restauración y validando que se pueda operar con la información contenida en ellos.

Gráfico 7. Respaldos. Elaborado por Pablo Corona, adaptación de @ pcoronaf

5.1.7 Cifrado

El cifrado es una herramienta importante para proteger la información confidencial. Convierte los datos en un formato ilegible para aquellos que no tienen la clave de cifrado correcta. Ayuda a proteger los datos aplicando un algoritmo que los desarticula, de manera que los datos sólo pueden ser recuperados al someterlos a un proceso de descifrado con la clave correspondiente.

Por ejemplo, existe el cifrado en reposo que es una técnica que se utiliza para proteger la información mientras está almacenada en dispositivos de almacenamiento, como discos duros, unidades USB o servidores. En caso de que un dispositivo de almacenamiento sea robado o extraviado, el cifrado en reposo garantiza que los datos almacenados en el dispositivo no puedan ser accedidos por terceros no autorizados. Además, es un requisito legal en muchos países para proteger la privacidad de la información personal. Para implementar el cifrado en reposo es necesario utilizar herramientas y software de cifrado, como BitLocker en Windows o FileVault en macOS.

El caso del ataque a un sitio web de encuentros extramatrimoniales pone en evidencia la importancia de contar con un sistema de cifrado de datos sobre todo cuando, como en este caso, se trata de información sensible.

Caso 4. Ciberataque de sitio web de encuentros extramatrimoniales (2015)

En julio de 2015 un sitio web dedicado a facilitar encuentros extramatrimoniales fue víctima de un ciberataque masivo. Los atacantes, autodenominados "The Impact Team", afirmaron haber comprometido la base de datos de la empresa y obtener acceso a una gran cantidad de información confidencial de sus usuarios. El incidente resultó en la filtración de datos personales y confidenciales de millones de usuarios, incluyendo nombres, direcciones de correo electrónico, números de teléfono y detalles de las transacciones realizadas en el sitio. Además, los atacantes amenazaron con publicar esta información en línea si la empresa y otros sitios relacionados no eran cerrados.

Este incidente generó una amplia cobertura mediática y tuvo un impacto significativo, tanto para los usuarios afectados como para la reputación de la empresa. Al no pagar el rescate exigido, datos de 32 millones de usuarios del portal fueron publicados, incluyendo sus nombres, preferencias sexuales, direcciones y números de tarjetas de crédito. A parte del impacto grave en las vidas personales de los usuarios, resultando en al menos dos suicidios a partir de la filtración, la publicación planteó riesgos de seguridad para los usuarios identificables cuyo comportamiento era punible en sus países. Como consecuencia de lo anterior, el CEO de la empresa se vio forzado a renunciar.

Posteriormente, se llevaron a cabo investigaciones sobre el evento y se identificó que las prácticas de seguridad de la empresa eran deficientes, incluyendo la falta de encriptación adecuada de los datos de los usuarios. El incidente destacó la importancia de implementar medidas de seguridad robustas, como el uso de encriptación y la gestión adecuada de la información personal y confidencial para proteger los datos de los usuarios.

6. Servicios en la nube

Entre las herramientas de trabajo en el ámbito digital que más se han ido expandiendo y son utilizados por cada vez más empresas están los servicios en la nube. Estos ofrecen extensos beneficios debido al dinamismo y maleabilidad que brindan a las empresas, pues ya no tienen que comprar hardware ni aprovisionarlo. Adicionalmente, los servicios de nube minimizan el tiempo de inactividad y permiten reducir costos.

La nube también ofrece algunos beneficios de seguridad; de hecho, los servicios en la nube han demostrado ser una herramienta valiosa para proteger a las empresas privadas contra los ciberataques. Al contar con estos servicios, las empresas pueden aprovechar el *hardening* de la infraestructura y las medidas de seguridad implementadas por proveedores confiables. Más adelante veremos cómo el *hardening* en la nube ha ayudado a prevenir incidentes y cómo las empresas han utilizado los servicios en la nube para mitigar los efectos adversos de los ciberataques. Sin embargo, cabe recordar que estos beneficios sólo son aplicables si se comprenden y adoptan modelos nativos de la nube, y se acondicionan sus arquitecturas y controles para ajustarse a los atributos y las condiciones de las plataformas en la nube.

6.1 ¿Qué tipos de nube existen?

Modelos de servicio en la nube

La nube se puede definir con base en tres modelos de servicio fundamentales. El Software como Servicio (SaaS) es una aplicación completa administrada y alojada por el proveedor de servicio de nube. Se puede acceder a esta aplicación por medio de un navegador web, una aplicación móvil o una aplicación de cliente. En contraste, la Plataforma como Servicio (PaaS) proporciona plataformas de desarrollo como bases de datos, plataformas de almacenamiento de archivos y colaboración, o incluso procesamiento de aplicaciones propietarias. En este modelo, no se manejan redes u otra infraestructura subyacente. Finalmente, la Infraestructura como Servicio (IaaS) permite acceder a un conjunto de recursos de infraestructura base de informática, como red o almacenamiento. Los servicios de nube pueden caer en más de uno de los modelos mencionados.

Modelos de implementación de la nube

Hay cuatro modelos de implementación en la nube que se basan en las tecnologías

	Administrada por	Infraestructura propiedad de	Infraestructura localizada en	Accesible y consumida por
Pública	Proveedor externo	Proveedor externo	Instalación propia	No confiable
Privada/ Comunitaria	Organización / Proveedor ext.	Organización / Proveedor ext.	Instalación propia / Instalación externa	Confiable
Híbrida	Organización y proveedor ext.	Organización y proveedor ext.	Instalación propia y externa	Confiable y no confiable

Gráfico 8. Nube híbrida y nube privada. Elaborado por Pablo Corona.

implementadas y consumidas. Se pueden diferenciar conforme a su administración, la propiedad y localización de la infraestructura, así como su confiabilidad, tal como se puede apreciar en el siguiente gráfico.

6.2 Alcance y responsabilidades de la seguridad en la nube

La seguridad en la nube y su cumplimiento conllevan todo de lo que un equipo de seguridad es responsable hoy en día, aplicado a la nube. Todos los dominios de seguridad tradicionales permanecen, pero la **naturaleza de los riesgos, roles y responsabilidades, y la implementación de los controles** cambian. Las responsabilidades de seguridad también se dividen entre las organizaciones y el proveedor del servicio de nube. Lo anterior es conocido como el **modelo de responsabilidad compartida (gráfico 9).**

La responsabilidad de la seguridad va ligada al nivel de dominio que se tiene sobre la arquitectura:

- **Software como Servicio (SaaS):** La responsabilidad de casi toda la seguridad recae en el proveedor del servicio de nube. El usuario sólo puede acceder y gestionar el uso de la aplicación.
- **Plataforma como Servicio (PaaS):** Las responsabilidades de seguridad se dividen de manera más equitativa. La seguridad de la plataforma es responsabilidad del proveedor del servicio de nube. El consumidor/usuario adquiere responsabilidad de todo lo que sea implementado en la plataforma, incluyendo características de seguridad.
- **Infraestructura como Servicio (IaaS):** Este modelo otorga mucha más responsabilidad al cliente. Aquí, el proveedor se responsabiliza de la seguridad de base, mientras el usuario es responsable de todo lo que compone la infraestructura.

Responsabilidad	IaaS	PaaS	SaaS
Contenido	■	■	■
Políticas de acceso	■	■	■
Uso	■	■	■
Despliegue	■	■	
Seguridad de aplicaciones web	■	■	
Identidad	■		
Operaciones	■		
Acceso y autenticación	■		
Seguridad de red	■		
Datos, contenido y sistemas alojados	■		
Bitácoras de auditoría			
Red			
Almacenamiento y cifrad			
Comunicación entre procesos y hardening del kernel			
Arranque			
Hardware			

■ Responsabilidad del proveedor de servicios de nube
■ Responsabilidad del Usuario de nube

Gráfico 10. Responsabilidad según el modelo de servicio de nube. Elaborado por Pablo Corona.

Gráfico 9. Modelo de responsabilidad compartida. Elaborado por Pablo Corona.

Lo más relevante de cualquier proyecto en la nube es definir exactamente quién es responsable de cada porción de la seguridad para no dejar lagunas desatendidas. Es por ello que resulta importante saber qué control de seguridad específico ofrece un proveedor de servicios en la nube y qué tanto se adapta con él a los procesos y controles de la organización. El modelo de responsabilidad compartida se correlaciona de manera directa con dos recomendaciones:

- Los controles de seguridad internos deben ser diseñados, documentados e implementados por los proveedores de servicio con la finalidad que el usuario sea capaz de tomar decisiones informadas.
- Para cualquier proyecto en la nube, los usuarios deben crear una matriz de responsabilidades para documentar quién está implementando qué controles y cómo.

6.3 *Hardening* en la nube

Las principales responsabilidades en un entorno de nube son el mantenimiento y el hardening de las máquinas virtuales (VMs, por sus siglas en inglés) y los contenedores que se están operando, en especial en los servicios de tipo IaaS y/o PaaS. Por lo mismo, se debe considerar una serie de principios:

- Utilizar sistemas operativos de VM o imágenes reforzadas; se debe contar además con scripts de referencia para hardening del sistema operativo y recursos adicionales, así como un catálogo de servicios recomendados en la nube que se haya evaluado previamente para garantizar que cumpla con los requisitos de seguridad.
- Emplear alguna herramienta de aprovisionamiento de software, gestión de configuración e implementación de aplicaciones que ofrezca arquitecturas de referencia para diferentes servicios en la nube, como contenedores, clústeres y servidores.
- Buscar que los proveedores de nube puedan administrar y proteger los sistemas operativos host, o hipervisor, de la infraestructura subyacente. De esta manera, no mantienen el sistema operativo en sus máquinas virtuales.
- Tener configurada una cuenta de emergencia que pueda acceder de forma privilegiada a los activos en la nube, en caso de que no puedan ser utilizadas cuentas privilegiadas normales.
- Configurar la autenticación a través de 2FA para que sólo pueda acceder un grupo limitado de usuarios confiables.
- Configurar la herramienta o el ambiente de nube para que los respaldos de información y logs sean almacenados de preferencia fuera de la nube o, por lo menos, en algún servicio de nube diferente.
- Asegurarse de que las conexiones de red entre los proveedores de servicios de nube y el cliente estén establecidas por medio de soluciones VPN, limitando el acceso a un cierto número de direcciones IP.

Si los proveedores y usuarios de la nube logran implementar estas acciones y cuentan con una división de responsabilidades clara, la utilización de servicios en la nube puede brindar considerables beneficios en materia de ciberseguridad. El caso del ciberataque a una plataforma de desarrollo de software colaborativo en 2018 nos muestra cómo la utilización de servicios de nube hubiera podido prevenir los daños causados.

Caso 5. Ataque DDoS a una empresa de desarrollo y servicios de software (2018)

En 2018 una empresa fue objeto de un ataque DDoS (Distributed Denial of Service) que afectó su disponibilidad y funcionamiento. Durante varios días experimentó interrupciones en sus servicios debido a la gran cantidad de tráfico malicioso dirigido hacia su infraestructura. El ataque fue llevado a cabo por un grupo de ciberdelincuentes que utilizó una botnet para inundar los servidores de la compañía con una gran cantidad de solicitudes falsas. Esto provocó una sobrecarga en los sistemas, lo que resultó en la caída de los servicios y dificultades de acceso para los usuarios legítimos.

Este ataque tuvo varios impactos significativos para la empresa. En primer lugar, la interrupción del servicio, lo que afectó negativamente a los desarrolladores y usuarios que dependían de la plataforma para gestionar sus proyectos. Además, su reputación se vio afectada debido a la incapacidad de proporcionar un servicio confiable durante el periodo del ataque.

En respuesta, la plataforma desplegó sistemas de mitigación de DDoS y aumentó la capacidad de sus servidores y la colaboración con proveedores de servicios de seguridad cibernética. Estas medidas le permitieron restablecer poco a poco sus servicios y protegerse contra futuros ataques similares.

En este caso, la utilización de servicios de nube hubiera podido ayudar a prevenir el ataque a la empresa tras haber aprovechado la infraestructura y las herramientas de mitigación de DDoS proporcionadas por el proveedor. Estos servicios suelen incluir sistemas de detección y mitigación de DDoS avanzados, balanceo de carga para distribuir el tráfico de manera equitativa y redundancia en la infraestructura para garantizar la disponibilidad continua del servicio, incluso durante un ataque.

Por otro lado, los servicios en la nube pueden proporcionar capacidades de monitoreo y análisis de datos en tiempo real para detectar patrones anómalos en el tráfico de datos. Esto permite identificar actividades sospechosas o ataques en curso y responder de manera proactiva. Asimismo, almacenar copias de respaldo de los datos de los dispositivos IoT en la nube permite restaurar con mayor rapidez la funcionalidad de los dispositivos después de un ataque o una interrupción.

6.4 Particularidades de respuesta ante incidentes en la nube

La respuesta ante incidentes es un elemento fundamental en todo proyecto que implique la seguridad de la información. La mayoría de las empresas cuenta con algún plan de respuesta ante incidentes para definir cómo se analizará un ataque. Debido a que la nube manifiesta diferencias en el acceso y gestión de la información, las organizaciones deben adaptar sus protocolos de seguridad.

Cualquier incidente que implique a un proveedor de nube pública exigirá la comprensión de los acuerdos de nivel de servicio (conocidos en inglés como Service Level Agreements o SLAs). Los SLAs de cada proveedor de servicios en la nube deben garantizar el soporte a las tareas de gestión de incidentes requeridas para una ejecución efectiva del plan de respuesta ante incidentes corporativos. Debido a lo anterior, es primordial comprobar los procedimientos con el proveedor de servicios de nube, garantizando que este tenga los contactos necesarios de la organización para notificar cuando se detecte un incidente.

Para más información sobre la respuesta a incidentes consulta el capítulo 8 de esta guía.

7. Ciberseguridad industrial

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 sistemas industriales. Con el aumento del uso de dispositivos Internet de las Cosas (IoT, 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.

© Noob/Freepik

De manera general, IoT es un término que se refiere a la interconexión de objetos cotidianos a internet permitiéndoles enviar y recibir datos, idealmente en tiempo real. La idea detrás de IoT es permitir que los objetos interactúen entre sí y con el entorno, creando una red global de dispositivos interconectados que puedan ser controlados y monitoreados de manera remota.

El Internet Industrial de las Cosas (IIoT, por sus siglas en inglés) es un subconjunto de la IoT. El término se refiere a la tecnología IoT utilizada en los procesos de manufactura y es una tecnología crucial para la Industria 4.0. La IIoT puede tener muchos de los mismos usos y beneficios que la IoT, sólo que el nivel de especialización y características de construcción y operación de los dispositivos son mucho más robustos. Puede integrar sensores inteligentes en maquinaria de fabricación, sistemas de energía o en infraestructuras como tuberías y cableado. Gracias a los datos que recopilan y a su funcionalidad avanzada, estos sensores pueden ayudar a las empresas industriales a aumentar su eficiencia, productividad, la seguridad de los empleados y mucho más. A diferencia de la IoT general, la IIoT se centra menos en el usuario y más en el proceso; asimismo, los dispositivos finales suelen estar integrados en la maquinaria y en otros activos de producción.

Los Sistemas de Control Industrial, por otro lado, son sistemas utilizados para controlar y monitorear los procesos industriales. Estos incluyen PLC (controladores lógicos programables), DCS (sistemas de control de procesos) y SCADA (sistemas de supervisión y control de procesos a distancia). Al igual que los dispositivos IoT, también son vulnerables a ataques cibernéticos debido a su conectividad a internet.

7.1 Riesgos particulares de los sistemas de TO

Recordando las diferencias entre las prioridades de ciberseguridad en sistemas de TI y TO, uno de los mayores riesgos de seguridad cibernética en el ámbito industrial es la posibilidad de que los atacantes accedan a los sistemas y causen una interrupción en los procesos industriales. Esto podría tener consecuencias graves, como paros en la producción, pérdida de datos y daños físicos a la maquinaria o incluso a las personas y al medio ambiente. Además, los atacantes podrían utilizar los sistemas ya comprometidos para espiar, robar información confidencial o incluso conocer a detalle los procesos productivos de las empresas.

Para protegerse contra estos riesgos es esencial contar con medidas de seguridad cibernética en los dispositivos IoT y los Sistemas de Control Industrial. Esto incluye, entre otros, la implementación de firewalls, la actualización regular de software y la configuración segura de los dispositivos. También es importante garantizar que sólo los usuarios autorizados tengan acceso a los sistemas y que se cuente con medidas de seguridad adicionales, como el

cifrado de datos y la autenticación de usuarios. A parte de la implementación de medidas de seguridad, es crucial que las empresas industriales realicen pruebas de seguridad cibernética con regularidad para detectar y corregir vulnerabilidades en los sistemas, un proceso mejor conocido en la industria como "análisis de vulnerabilidades".

7.2 Recomendaciones de seguridad para dispositivos IoT y dispositivos de control industrial (ICS)

Con respecto a los dispositivos IoT y TO utilizados para el control y la automatización industrial, podemos citar una serie de recomendaciones sobre medidas de ciberseguridad específicas, las cuales en muchos de los casos no requieren una inversión monetaria muy grande. Asimismo, muchas de ellas son escalables, de manera que la inversión inicial es manejable.

La seguridad de la red industrial involucra la protección de las redes de automatización contra el acceso no autorizado, así como el control de todas las interfaces con otras redes, tales como el conducto a la red de la oficina. En particular en este contexto deben protegerse los gateways de mantenimiento remoto a internet. La protección de las comunicaciones contra la intercepción y la manipulación mediante la transmisión de datos cifrados y la autenticación de los nodos de comunicación es fundamental y parte de una estrategia de ciberseguridad integral.

Algunas de las acciones que las empresas pueden tomar para proteger las redes industriales son:

1. Implementar un sistema de gestión de identidad y acceso (IAM – Identity and Access Management) para controlar quién tiene acceso a los dispositivos IoT e ICS y a los datos que estos recogen.
2. Configurar los dispositivos IoT e ICS para que sólo se comuniquen con servidores y dispositivos autorizados.
3. Utilizar cifrado de extremo a extremo para proteger los datos que se transmiten a través de los dispositivos IoT e ICS.
4. Segregar las redes industriales de las redes de oficina para evitar la propagación de una infección. Asimismo, asegurar que los dispositivos IoT e ICS estén aislados de la red principal de la empresa.
5. Actualizar regularmente el software de los dispositivos IoT e ICS para garantizar que estén protegidos contra las últimas amenazas de seguridad.
6. Usar un *firewall* para proteger los dispositivos IoT e ICS contra ataques externos.
7. Utilizar un sistema de detección y respuesta de incidentes (SIEM, por sus siglas en inglés) para detectar y responder rápidamente ante cualquier incidente de seguridad, así como sistemas de detección y prevención de intrusiones (IDS/IPS, por sus siglas en inglés) para detectar y bloquear ataques externos a las redes industriales.
8. Realizar pruebas de penetración con regularidad para detectar vulnerabilidades en los dispositivos IoT e ICS.
9. Ejecutar pruebas de penetración con frecuencia para detectar vulnerabilidades en las redes industriales.
10. Capacitar al personal en materia de ciberseguridad y sobre la importancia de seguir las mejores prácticas de seguridad al utilizar dispositivos IoT e ICS.
11. Implementar un plan de continuidad del negocio y un plan de respuesta a incidentes para garantizar la capacidad de recuperación en caso de un ataque exitoso.

En el contexto industrial, la ciberseguridad es esencial para todo tipo de empresas, especialmente con la creciente dependencia de los Sistemas de Control Industrial en las tecnologías de la información. Los ataques cibernéticos pueden tener graves consecuencias para la operación de una industria y poner en riesgo la seguridad y la vida de los trabajadores y la población en general.

Por ello, es crucial tomar medidas de protección contra los ataques de ciberseguridad, como la implementación de soluciones de seguridad, la capacitación del personal y la realización de evaluaciones regulares en esta materia. Al adoptar prácticas de seguridad sólidas y efectivas se puede minimizar el riesgo de ataques cibernéticos y garantizar la continuidad de la operación.

En el sector industrial, la seguridad cibernética es de vital importancia para proteger los dispositivos IoT y de control industrial (ICS) contra los ciberataques. La aplicación de medidas de seguridad adecuadas puede prevenir incidentes graves y salvaguardar los sistemas y procesos industriales. En esta sección presentamos el caso de un ciberataque a una planta petroquímica que ilustra los peligros particulares que surgen en el caso de los ciberataques a la TO, a diferencia de los ataques a la TI, y cómo la implementación de los controles listados arriba hubiera podido evitar o mitigar el daño causado.

Caso 6. Ataque a la planta petroquímica de Arabia Saudita (2012)

En 2012, la compañía petrolera estatal de Arabia Saudita sufrió un ataque devastador que afectó a sus Sistemas de Control Industrial y provocó la interrupción de las operaciones. Los atacantes utilizaron un *malware*, conocido como "Shamoon", para infectar miles de computadoras en la red de la compañía, borrando datos y dejando inoperativos los sistemas durante varios días. El *malware* se propagó rápidamente y causó la destrucción masiva de datos en las máquinas infectadas, lo que llevó a la inutilización de miles de sistemas y servidores.

El resultado fue una interrupción significativa en las operaciones de la petrolera, incluyendo el acceso a datos y la comunicación interna. El incidente también afectó a la infraestructura crítica de la compañía, lo que implicó una disminución en la producción y el cierre temporal de algunas operaciones.

En este caso pudieron haberse aplicado diversas recomendaciones de seguridad para dispositivos IoT y dispositivos de control industrial (ICS) para así prevenir o mitigar el impacto del incidente. Entre ellas podríamos destacar:

Segmentación de redes: Separar las redes de los dispositivos IoT y los dispositivos de control industrial del resto de la infraestructura de TI de la planta. Esto hubiera ayudado a evitar que un ataque dirigido a estos dispositivos se propagara a otros sistemas, y a limitar el impacto en caso de compromiso.

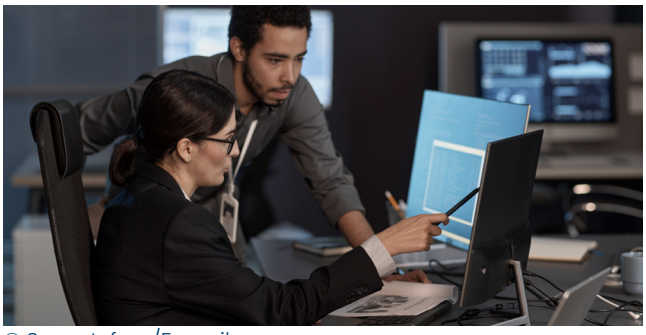
Monitoreo y detección de anomalías: Implementar soluciones de monitoreo y detección de intrusiones para identificar actividades sospechosas o anómalas en tiempo real. Esto habría permitido una respuesta temprana ante posibles ataques o brechas de seguridad.

Actualizaciones y parches regulares: Mantener los dispositivos IoT y los dispositivos de control industrial al día con las últimas actualizaciones y parches de seguridad. Esto ayudaría a mitigar las vulnerabilidades conocidas y a corregir posibles fallas de seguridad.

Evaluación de proveedores y cadenas de suministro: Realizar una evaluación exhaustiva de los proveedores de dispositivos IoT y dispositivos de control industrial para garantizar que cumplan con los estándares de seguridad requeridos. Es importante establecer medidas de seguridad en la cadena de suministro para prevenir la introducción de dispositivos comprometidos o modificados maliciosamente.

8. Gestión de incidentes

A pesar de todas las medidas de prevención que podamos 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 otorgan acceso a la información almacenada en dispositivos físicos o virtuales a una persona o grupo de personas no acreditadas.


© Seventyfour/Freepik

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 el apoyo de áreas como recursos humanos, sistemas y el departamento legal de la organización.

Los estándares y directrices internacionales juegan un papel importante para poder establecer acciones de respuesta ante incidentes en las empresas. El National Institute of Standards and Technology (NIST) de Estados Unidos cuenta con la "Guía para el Manejo de Incidentes de Seguridad (SP 800-61)"; esta es de acceso público y es reconocida como una referencia en el manejo de incidentes de seguridad informáticos. Además, nos podemos apoyar en el estándar internacional ISO/IEC 27001 que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información. También el estándar internacional ISO/IEC 27002 se enfoca en la seguridad de la información y actualmente se ve como un complemento a la norma ISO/IEC 27001. Otro estándar internacional relevante es el ISO 22301; se trata del primer estándar internacional para la Gestión de Continuidad del Negocio (BCM), desarrollado para ayudar a las organizaciones a minimizar el riesgo del cese de las actividades ante los incidentes de seguridad de la información.

Una herramienta complementaria, útil y accesible que muestra posibles medidas ante distintos tipos de incidentes son los *playbooks*. Estos se pueden encontrar de forma pública en internet y definen las líneas de acción a seguir ante incidentes. Pueden ayudar a evitar la toma de decisiones apresuradas, además de aportar elementos importantes de análisis para tener claridad en las opciones de mitigación de las amenazas críticas de la organización. Algunos de ellos están enfocados en atender un tipo de fallo en particular, como los de *Incident Response*[1], o en un tipo de ataque específico, como los de Rapid7.[2]

La preparación de un plan de respuesta ante incidentes usando estos recursos permitirá tener una rápida respuesta en caso de ocurrir un evento. Al no contar con un proceso de gestión de incidentes, exponemos nuestra empresa a riesgos graves, tal como ilustra el caso de una procesadora de carne.
En este capítulo revisaremos todas estas estrategias que, en su conjunto, permiten lograr una respuesta rápida y eficaz para mitigar posibles daños tras un ciberataque. Asimismo, discutiremos cómo identificar un incidente, cómo preparar un plan de respuesta ante este tipo de eventos y qué elementos debe contener, y cómo aprender de un ciberataque.

Caso 7. Hackeo a procesadora de carne (2021)

En mayo de 2021, la empresa procesadora de carne más grande del mundo sufrió un grave ciberataque que afectó sus operaciones en Australia, Canadá y Estados Unidos. Los hackers lograron infiltrarse en las redes informáticas de la empresa mediante ransomware, exigiendo un rescate en criptomonedas para restaurar el acceso a sus sistemas.

A diferencia de otros casos donde las empresas han implementado una gestión de incidentes efectiva, la compañía no pudo evitar el ataque ni responder de manera adecuada. En lugar de contar con medidas preventivas y un plan de respuesta sólido, se vio obligada a pagar un rescate de $11 millones de dólares para recuperar el control de sus sistemas luego de que el ciberataque hubiera tenido un impacto significativo en sus operaciones.

El ataque tuvo un efecto devastador, al grado de que la compañía se vio obligada a detener temporalmente el sacrificio de ganado en todas sus plantas de Estados Unidos durante un día, lo que puso en peligro la cadena de suministro de alimentos y generó preocupaciones sobre posibles aumentos en los precios para los consumidores. Además del impacto económico, el ciberataque también afectó su reputación, a razón de que no pudo garantizar la seguridad de los datos de sus clientes y empleados, lo que podría haber erosionado la confianza del público y de sus socios comerciales.

Este evento muestra la importancia de implementar una sólida gestión de incidentes y tener medidas de seguridad cibernética adecuadas. La falta de una respuesta efectiva resultó en pérdidas financieras significativas, pagando una suma considerable como rescate, aunado al costo asociado con la interrupción de las operaciones.

Las siguientes estrategias de gestión de incidentes pudieron haber disminuido el riesgo y los daños por el ataque:

- **Plan de respuesta ante incidentes:** Tener un plan de respuesta a incidentes bien estructurado y actualizado habría permitido una acción temprana en caso de un ataque cibernético. Este plan debería incluir roles y responsabilidades claras para el equipo de respuesta a incidentes, procedimientos de comunicación interna y externa, y pasos específicos para contener y mitigar el ataque.
- **Monitoreo y detección temprana:** Contar con sistemas de monitoreo avanzados y soluciones de detección de amenazas habría permitido a la empresa identificar el ataque en una etapa temprana, lo que habría aumentado las posibilidades de detener la propagación del ransomware y minimizar los daños.
- **Comunicación efectiva:** En caso de un ataque cibernético es crucial mantener una comunicación clara y rápida con los empleados, clientes, socios comerciales y autoridades relevantes. Una respuesta transparente y oportuna puede ayudar a mitigar el impacto en la reputación y mantener la confianza de los stakeholders.
- **Coordinación con autoridades:** Trabajar en estrecha colaboración con las agencias de aplicación de la ley y las autoridades cibernéticas habría permitido a la compañía obtener asistencia en la investigación y el rastreo de los atacantes. Esto también podría haber aumentado las posibilidades de recuperar los datos y rastrear el origen del ataque.

8.1 ¿Cómo se puede reconocer un posible incidente?

Algunas formas comunes de identificar posibles amenazas incluyen, entre otras:

- Alertas de herramientas de monitoreo de seguridad.
- Mal funcionamiento o fallas dentro de los sistemas.
- Comportamientos inusuales.
- Modificaciones de archivos de forma inesperada.
- Intentos de filtraciones.
- Informes de usuarios con configuraciones diferentes a las otorgadas por el equipo de tecnologías de la información.
- Descontrol en el acceso de los administradores de sistemas o redes.
- Reportes de personas externas en áreas restringidas por el personal de seguridad.
- Faltas de actualizaciones en los sistemas operativos.
- Software que no cuenta con licencia.
- Múltiples intentos fallidos de inicio de sesión.
- Descargas de archivos grandes.
- Uso elevado de memoria.

8.2 ¿Cómo preparar un plan de respuesta ante incidentes?

Un plan de respuesta a incidentes documenta los pasos a seguir en caso de presentarse un ataque o cualquier otro incidente de seguridad de la información. Cada organización debe tener un plan cuyo diseño tome en cuenta su propio entorno real (activos de hardware, de software, personal, necesidades, tipo de información manejada, etc.); este debe ser fácil de entender e implementar, y alinearse con otros planes y políticas de la empresa. Su preparación incluye el desarrollo de documentación con información relevante, donde se debe mencionar a las personas que participarán en los procedimientos y las actividades que deben ejecutarse para abordar el incidente.

Entre las partes fundamentales del plan de respuesta a incidentes destacan el nombramiento del equipo y de los individuos responsables, la definición de lo que se considera un incidente, la identificación de sistemas que contienen información crítica, los mecanismos de documentación de evidencia que se usarán, y el proceso de escalación que se seguirá en caso de incidentes.

Una vez desarrollado, este plan debe ser ejecutado en una simulación; con esto se validará su funcionamiento en caso de una crisis. Se recomienda realizarle actualizaciones constantes que abarquen cambios en la información, compromisos contractuales, necesidades de los clientes o normativa aplicable a la organización con el fin de garantizar que sea válido y eficaz.

8.2.1 Contención y eliminación de amenazas y recuperación

La contención y eliminación de amenazas es el primer paso que se debe dar ante un incidente para bloquear la propagación del ataque y restaurar los sistemas. El equipo de respuesta de incidentes deberá eliminar todas las amenazas bloqueando o desconectando los sistemas comprometidos, asegurándose de limpiar el malware o virus, bloqueando a los usuarios maliciosos o comprometidos y, de ser posible, restaurando los servicios empezando por los críticos. Sin embargo, antes de limpiar los sistemas es importante conservar una copia del estado de los sistemas afectados para poder proceder con el análisis forense.

8.2.2 Análisis forense

Para conocer el impacto y determinar los riegos asociados en caso de un incidente de seguridad de la información, es necesario comenzar de forma inmediata un análisis forense tras la contención. Este ayuda a conocer más a detalle lo sucedido durante el evento y así poder mitigar los riesgos y vulnerabilidades de la organización.

Un punto crítico para el éxito de la investigación realizada durante el análisis forense será la

definición correcta de las personas que ejecutarán la investigación. Generalmente el equipo se encuentra conformado por personal técnico del área de sistemas o tecnologías de la información, pero siempre es de ayuda contar con la colaboración de al menos una persona del área de recursos humanos, así como de algún integrante del equipo legal, con la finalidad de identificar los posibles riesgos legales asociados.

8.2.3 Trazar el origen del incidente

El análisis debe iniciar con la documentación de todas las acciones y antecedentes que preceden a la detección del incidente. Se busca responder a las preguntas básicas de: ¿cuándo fue detectado?, ¿quién lo detectó?, ¿hay comunicación de algún tercero solicitando un rescate o pago? El resultado de esta documentación abrirá posibles rutas a seguir.

Los equipos técnicos harán un escaneo de la red e identificarán topologías, equipos afectados, UMT, computadoras, *routers, switches, firewalls,* proxy, IDS's y dispositivos de almacenamiento. Todo esto debe registrarse como comprometido, aislarse y conocer la situación de cada uno, cambiando los accesos de administración de forma inmediata. Este equipo técnico también deberá realizar una recuperación de bitácoras de todos los dispositivos de red, comunicación y servidores. Debe revisar las memorias caché de los sistemas, los archivos temporales y el registro de sucesos de cada dispositivo disponible pues podrían aportar información relevante sobre cómo dio inicio el evento y cuál fue el posible punto de vulneración usado.

8.2.4 Análisis de impacto

La investigación debe analizar cuál es la situación actual con hechos y partes afectadas, y evaluar el nivel de gravedad. En caso de haber afectaciones, se señalará la infraestructura comprometida; esto incluye computadoras, servidores físicos y virtuales, así como medios de almacenamiento físicos y virtuales. Es importante identificar la información contenida en estos y si pudo haber sido expuesta; asimismo, examinar si se trataría de datos de tipo personal o confidencial, si pertenecen a la empresa o si se trata de información de clientes y proveedores.

Para minimizar el riesgo en estos casos, se recomienda solicitar el apoyo del equipo legal, ya que pudiera ser necesario comunicar a clientes, proveedores o autoridades sobre la ocurrencia del incidente. Otro punto clave es conocer los costos asociados con pérdidas de equipo y servidores, así como los costos de los servicios de los equipos especializados en recuperación, análisis forense y legal, en caso de ser necesarios. En la investigación se debe incluir la información de dispositivos contratados con externos, nubes públicas o privadas, espacios de almacenamiento, servidores, etc.

8.2.5 Documentación de evidencia

Para el respaldo de la investigación es necesario realizar una copia imagen de todos los ambientes. La organización debe evaluar si cuenta con herramientas para desarrollarlo o si es necesario contratar a un tercero especializado en el tema. Se recomienda que el análisis y la investigación se efectúen sobre estas copias.

Se debe llevar una bitácora estricta y detallada de los accesos y tareas realizadas en las copias de respaldo forense, con el fin de no contaminar o manipular evidencia de forma incorrecta. Esta investigación también debe revelar si hay personal interno en la organización que pudiera estar implicado; para evaluar el tema se debe tener entrevistas con el personal. Otro de los puntos a considerar y validar son las configuraciones de los equipos, pues es común que las personas detrás de la posible intrusión hayan realizado cambios con la finalidad de crear una vulneración más grande o de hacer más difícil de rastrear el punto de origen.

8.2.6 Reporte final

Es importante entregar un reporte final detallado con toda la información mencionada arriba que permita al Comité de Crisis dar una respuesta efectiva sobre el incidente. Este docu-

mento debe contar con conclusiones sobre el posible punto de inicio o paciente cero o si este ya fue confirmado, así como sobre la cantidad y tipo de información que quedó expuesta. El reporte se convertirá en una prueba, si es que se llega a tener algún proceso legal. Algunas partes fundamentales que debe abarcar son el objetivo del reporte, los emisores (del equipo o la empresa), un resumen de los incidentes, la evidencia (pantallas, muestra de logs, muestras de controles de accesos, contratos), metodologías y herramientas utilizadas en la investigación, así como las conclusiones de la misma.

8.2.7 Notificación de lo ocurrido

Usando el análisis forense, el Comité de Crisis deberá determinar las notificaciones necesarias. Si el incidente afecta datos personales que requieren notificar al Instituto Nacional de Transparencia (INAI), se recomienda que sea el equipo legal quien aborde este tema. Si la información comprometida está relacionada con datos del personal interno, se solicitará al equipo de recursos humanos que dé la notificación. Cuando se trate de datos sensibles de clientes, personal externo o proveedores, se debe evaluar en conjunto con el equipo legal cómo se dará el comunicado, ya que los contratos celebrados con cada uno pueden indicar formas diferentes de notificación, así como la penalización que se podría llegar a aplicar en cada caso.

8.2.8 Plan de Mitigación ante riesgos legales de un incidente de seguridad de la información

Es necesario que el equipo legal siempre forme parte de los Comités de Crisis y que, al igual que el equipo de tecnologías de la información, tenga claro qué afectaciones le toca aminorar. Los principales puntos de vulnerabilidad que las organizaciones deben cuidar para mitigar los posibles impactos legales en caso de un incidente son:

- **Contratos celebrados con proveedores, clientes y personal externo.** La organización debe incluir cláusulas de confidencialidad que expresen de forma clara cómo se debe de comunicar un incidente en caso de presentarse. Algunas empresas agregan penalizaciones fuertes en caso de incumplimiento.
- **Secretos industriales.** Cuando las organizaciones cuentan con información propia o de terceros que es considerada un secreto industrial, es recomendable resguardarla en lugares seguros e implementar mecanismos de seguridad tecnológica.[3]
- **Contratos de confidencialidad.** También conocidos como NDA (por sus siglas en inglés, Non-Disclosure Agreement), deben celebrarse o firmarse con empleados, personal externo, clientes y proveedores. En caso de una vulneración, estos documentos adquieren relevancia ya que pueden ser requeridos si se debe notificar sobre información personal o confidencial que se ha filtrado con ayuda de personal interno, externo o por consecuencia de fallas de algún servicio prestado por un tercero o proveedor.
- **Información bancaria.** Sabemos que si la información extraída pertenece a la organización, las consecuencias pueden ser desastrosas. Pero también hay legislación que pudiera llegar a aplicarse, como la Ley de Instituciones de Crédito, en caso de que por alguna razón nuestra empresa salvaguarde información bancaria de terceros.
- **Información personal**. Las organizaciones tienen una responsabilidad de protección sobre los datos personales que guardan. En México, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) junto con el INAI garantizan el derecho de protección de datos personales. La LFPDPPP indica varias sanciones por incumplimiento y falta de diligencia.

8.2.9 Medidas posteriores

Es muy común que una vez finalizado el incidente los equipos se pregunten: ¿y ahora qué pasará? Lo ideal es aprender de estos infortunios. Los equipos deben analizar su solución de seguridad y abordar las vulnerabilidades detectadas. De hecho, las mejores prácticas nos sugieren

llevar una bitácora de dichas vulnerabilidades y de las soluciones aplicadas.
En todo caso, se recomienda documentar las lecciones aprendidas del proceso de respuesta al incidente, por ejemplo, en una base de datos. Analizar qué funcionó bien y qué se puede mejorar ante ataques en el futuro nos puede ayudar a ver dónde tenemos que reforzar nuestra estrategia de seguridad e identificar medidas de mejora que se pueden implementar. Algunas pueden incluir la implementación de nuevas soluciones de seguridad y monitoreo de amenazas internas y externas; capacitación al personal sobre amenazas de seguridad, como phishing, spam y malware; crear un documento sobre cómo escalar o con quién reportar cualquier posible infiltración o vulneración de forma oportuna; entre otras.

Es importante resaltar que el desarrollo de estrategias de ciberseguridad no es una tarea puntual sino cíclica, y su éxito depende de las revisiones periódicas y del aprovechamiento de cada incidente como una oportunidad para el aprendizaje. Sólo dándole esta continuidad a las acciones implementadas para fomentar la ciberseguridad en nuestra empresa podremos proteger nuestra información, nuestros sistemas, nuestra economía y nuestras relaciones con clientes y proveedores de manera oportuna frente a la diversidad de ciberamenazas que va evolucionando día con día.

9. Conclusión

En un mundo cada vez más digital y globalizado, la ciberseguridad se ha convertido en una preocupación fundamental para las empresas, especialmente para las PYMEs en México. Este documento ha sido el resultado de una colaboración significativa entre expertos del Diálogo Mexicano - Alemán en Infraestructura de la Calidad, y representa un esfuerzo conjunto para abordar los desafíos de la ciberseguridad en las cadenas globales de valor.

El intercambio continuo de datos y la creciente aplicación de soluciones de Industria 4.0 han mejorado la eficiencia de los procesos operativos, pero al mismo tiempo han aumentado los riesgos en el ámbito de la ciberseguridad. Las estadísticas revelan que México no está exento de estos riesgos, ocupando el tercer lugar en ciberataques en América Latina.

Los ciberataques pueden tener un impacto devastador en la economía de una empresa y su reputación. Esto es particularmente relevante para las PYMEs, que a menudo carecen de los recursos para obtener certificaciones en estándares internacionales o para contratar personal especializado en ciberseguridad, y por ello, se han convertido en un blanco popular para los cibercriminales. Partiendo de este contexto, el documento presente, junto con otras publicaciones de esta serie, busca proporcionar recomendaciones concretas para las PYMEs en México, ofreciendo una guía de implementación de políticas de ciberseguridad alineada con estándares internacionales.

Abarcando desde la definición de conceptos básicos hasta la gestión de riesgos, herramientas de protección, y medidas para la seguridad de la información en la nube y en el entorno industrial, este documento presenta una guía completa para mejorar la ciberseguridad empresarial. Su estructura modular permite a las empresas adaptar estas recomendaciones a sus necesidades específicas.

© Jackie_niam/Freepik

En resumen, la ciberseguridad es un desafío que no puede ser pasado por alto en el entorno empresarial actual. Esta guía es un paso importante para equipar a las PYMEs en México con los conocimientos y herramientas necesarios para proteger sus activos digitales y garantizar la continuidad de sus operaciones en un mundo cada vez más interconectado. La seguridad cibernética es un compromiso constante, y esta guía ofrece una base sólida para construir una estrategia de ciberseguridad efectiva y accesible acorde a las necesidades y los recursos de las PYMEs.

10. Referencias

[1] Disponible en
[2] Disponible en
[3] El uso, transmisión y/o difusión de secretos industriales es un delito con fundamentos legales en la Ley de la Propiedad Industrial, Ley del Procedimiento Administrativo, y en el Código Federal de Procedimientos Civiles.
[4] Aristegui noticias (2022). Más de 223 mil incidentes de seguridad cibernética de 2019 a la fecha: Guardia Nacional.
[5] Cámara de Diputados del H. Congreso de la Unión (2010). Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

[6] Centro de Innovación y Soluciones Empresariales (2022). ¿Qué es el hardening de sistemas operativos?
[7] Cybercrime Magazine (13 de noviembre de 2020). Cybercrime to Cost the World $10.5 Trillion Annually by 2025.
[8] Deloitte (2022). Cyber Security Landscape 2022.

[9] Expansión (2022). En un trimestre, México registró 80,000 millones de intentos de ciberataques.
[10] Guardia Nacional (2023). Manual Básico de Ciberseguridad para la Micro, Pequeña y Mediana Empresa MiPyME.
[11] Purplesec (2022). Vulnerability Scanning vs Penetration Testing.
[12] Saengphaibul V. (15 de marzo de 2022). A Brief History of the Evolution of Malware.
[13] Senadores Morena (2022). Buscan en el Senado crear marco jurídico para garantizar uso seguro de redes digitales.
[14] The World Bank (2022). Mexico Overview.
[15] Veracode (2022). Vulnerability Assessment and Penetration Testing.
[16] World Economic Forum (2022). The Global Risks Report 2022.