



SEGURIDAD
SECRETARÍA DE SEGURIDAD
Y PROTECCIÓN CIUDADANA



GN
GUARDIA
NACIONAL



CERT-MX

Centro Nacional de Respuesta
a Incidentes Cibernéticos

**Manual Básico de Ciberseguridad
para la Micro, Pequeña y Mediana
Empresa.**

Índice

1. Prólogo	03
2. Introducción	05
3. Elementos de Ciberseguridad para MiPyMEs	
3.1. Empleados	07
3.2. Seguridad en dispositivos móviles	11
3.3. Seguridad en la Red	15
3.4. Prevención de fraude electrónico	19
3.5. Privacidad y Seguridad de datos	23
3.6. Seguridad en los sistemas informáticos y sitios web	27
3.7. Seguridad en los servicios de correo electrónico	29
3.8. Políticas de seguridad	31
3.9. Respuesta a incidentes de seguridad	33
3.10. Seguridad de las operaciones	37
3.12. Seguridad en mecanismos de pago electrónico	41
3.11. Seguridad física	45
4. Glosario	48

1. Prólogo

El desarrollo de las Micro, Pequeñas y Medianas Empresas (MiPyMEs) resulta crucial para la economía de México, de acuerdo con el registro del Instituto Nacional de Estadística y Geografía (INEGI, 2016), las MiPyMEs representan el 99.8 por ciento de todas las empresas en el país, las cuales generan alrededor de 65 millones de empleos (72 por ciento del total en el país) y el 52 por ciento del Producto Interno Bruto (PIB).

Las MiPyMEs también han avanzado en la adopción de las tecnologías de la información y comunicación (TIC'S), incluyendo el Internet, para su operación, datos del INEGI señalan que más del 47 por ciento de las MiPyMEs se han vuelto dependientes de su uso.

En estas circunstancias, las MiPyMEs deben desarrollarse además del entorno económico al tecnológico, siendo éste último cada día objeto de ataques de la ciberdelincuencia ante las condiciones vulnerables en que se encuentran en este ámbito.

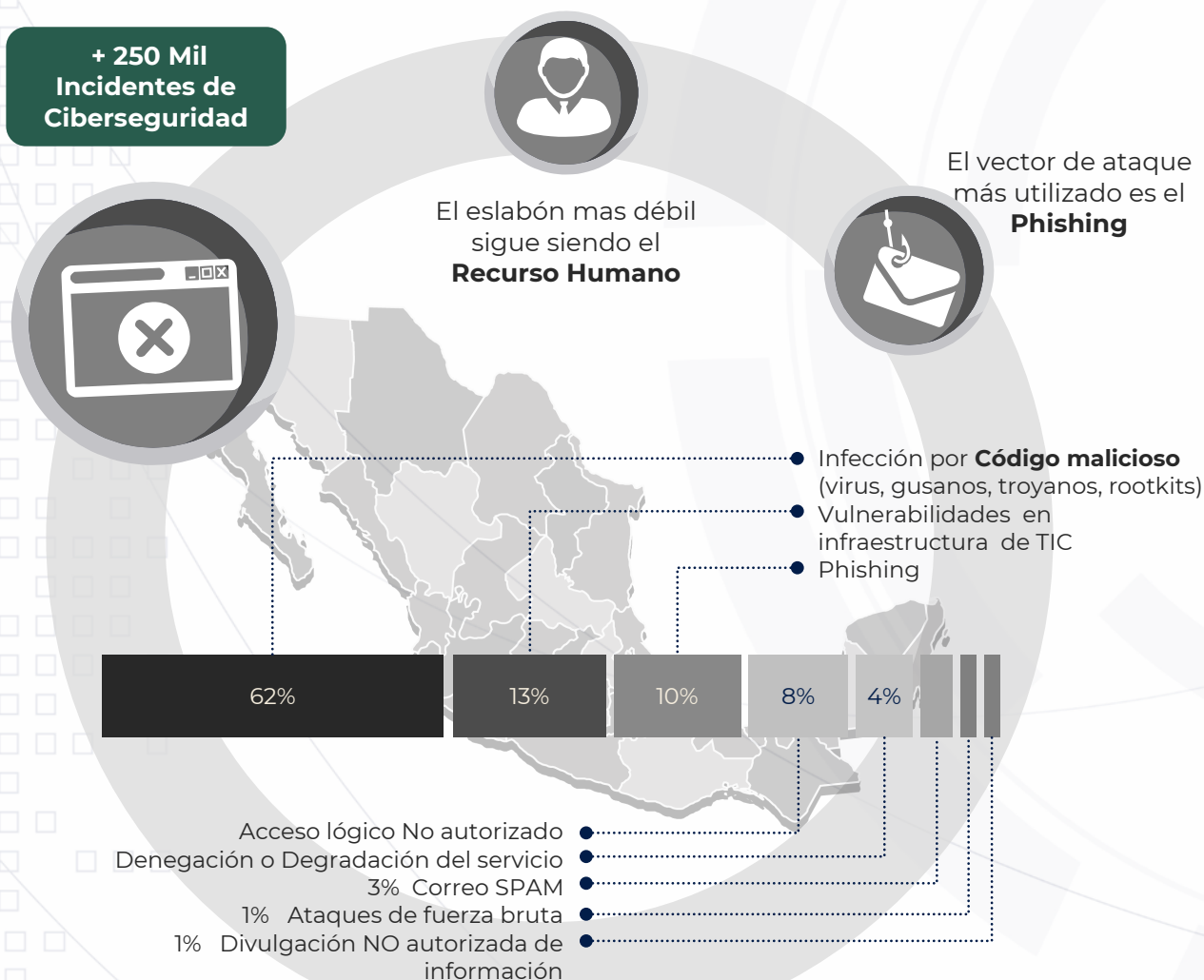
En nuestro país se ha incrementado el número de incidentes cibernéticos dirigidos a las empresas (entre ellas las MiPyMEs), registrándose por la Dirección General Científica de la Guardia Nacional un incremento de 142%, entre 2015 y 2017, superando los 16 mil novecientos eventos.

De acuerdo con reportes de la industria de seguridad informática, cada ataque cibernético exitoso dirigido a una PyME podría ocasionar en promedio una pérdida de 50 mil dólares, lo que para algunas significaría un daño que ocasionaría el cierre de la empresa.

A fin de proveer una herramienta práctica que permita incrementar la resiliencia cibernética de las MiPyMEs, la Guardia Nacional elaboró el presente “Manual Básico de Ciberseguridad para la Micro, Pequeña y Mediana Empresa (MiPyME)” con la finalidad de orientar a emprendedores (as) y empresarios (as) sobre buenas prácticas en la materia, que incluye además, recomendaciones para el debido cumplimiento de obligaciones respecto al manejo de información privada de acuerdo a las disposiciones aplicables.

Incidentes de Ciberseguridad registrados por la Guardia Nacional con impacto en México

Periodo diciembre 2012 — agosto 2018



Fuente: CERT-MX

2. Introducción

En este Manual Básico de Ciberseguridad, se mostrarán las principales líneas de acción propuestas para reducir los riesgos vinculados a las amenazas cibernéticas que puedan comprometer la seguridad de la información y fortalecer la ciberseguridad en las Micros, Pequeñas y Medianas Empresas (MiPyMEs). En el presente Manual se integran las mejores prácticas de ciberseguridad y modelos estratégicos basados en estándares internacionales. Los emprendedores y empresarios deberán considerar que la ciberseguridad es un trabajo constante que involucra procesos, tecnología y personas.

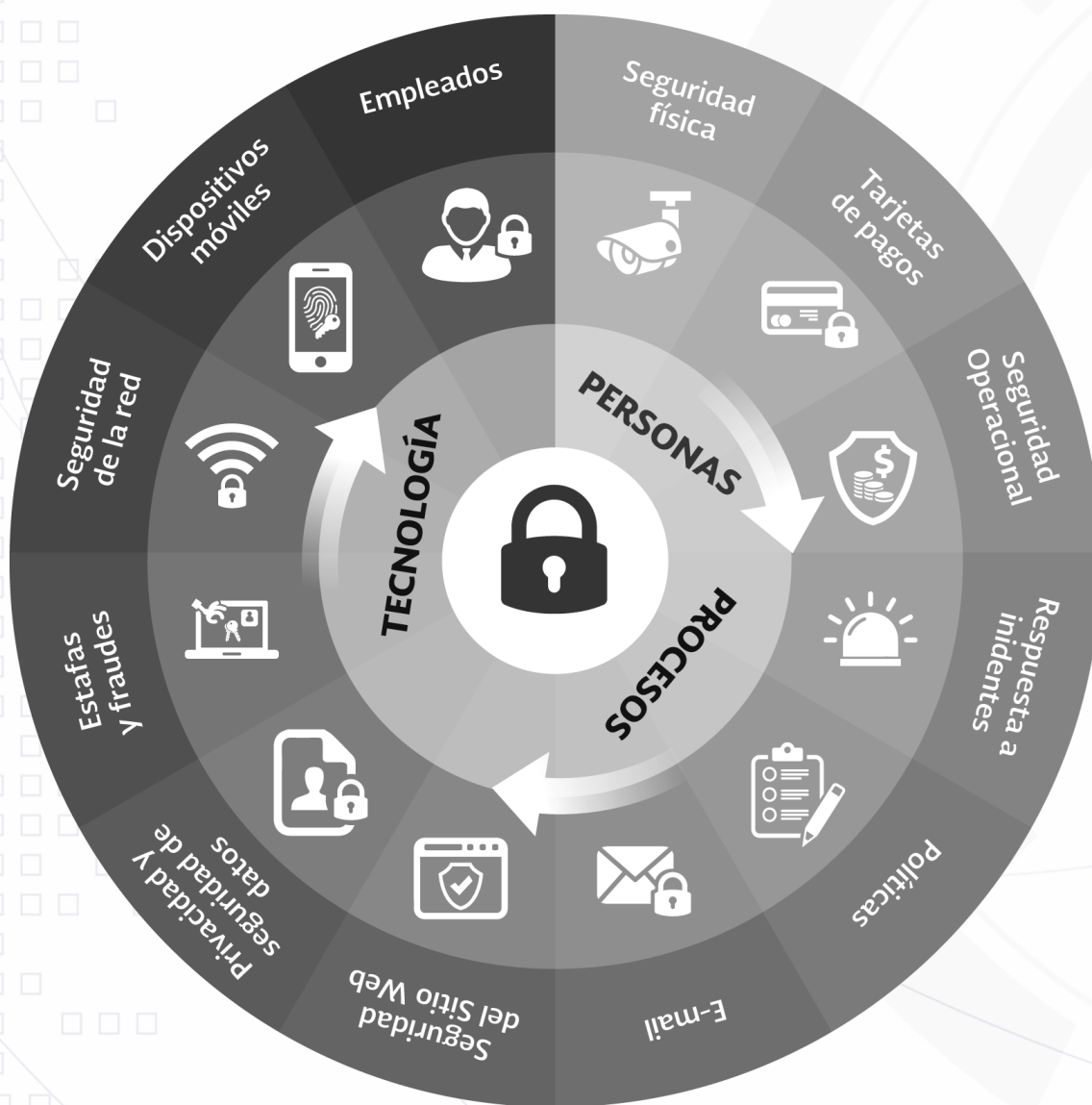
En ese sentido debe considerarse que la ciberseguridad es un término ampliamente definido, sin embargo lo establecido por la Unión Internacional de Telecomunicaciones (ITU, por sus siglas en inglés), en la Recomendación UIT-T X.1205, Unión Internacional de Telecomunicaciones, la describe como:

“Es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberespacio.”

De acuerdo con esta definición, las tareas de la ciberseguridad requieren del conocimiento de diversas disciplinas, el Manual Básico de Ciberseguridad presenta una serie de recomendaciones, buscando que la información resulte comprensible a emprendedores (as) y empresarios (as) para la identificación de riesgos y amenazas cibernéticas, así como de las medidas básicas para la protección de los activos y usuarios en el ciberespacio.

Entre las principales amenazas cibernéticas que podrían afectar a las MiPyMEs se encuentran el Phishing, la revelación de secretos comerciales, la venta fraudulenta de artículos o servicios y el mal uso y/o robo de información de datos personales, entre otras.

Cada una de las temáticas sugeridas están representados en el **Esquema “Elementos Básicos de Ciberseguridad para MiPyMEs”**:



3.1. Empleados



Las empresas deben establecer procesos formales de contratación para controlar y preservar la calidad de sus empleados. Muchos empleadores no cuentan con un proceso de reclutamiento idóneo para seleccionar a su personal con un perfil apto y confiable, lo que conlleva al riesgo de tomar decisiones de contratación imprudentes que pueden conducir a violencia en el lugar de trabajo, robo, malversación de fondos, demandas por contratación negligente, problemas derivados de la carencia de procesos bien definidos, y por último, generar responsabilidades para la organización.



Plan de acción de ciberseguridad

Empleados

Desarrollar un proceso de contratación que investigue adecuadamente a los candidatos.

El proceso de reclutamiento debe ser un esfuerzo de colaboración entre los diferentes grupos de su organización, incluidos el de recursos humanos, seguridad, legal y de gestión. Es importante contar con un proceso de contratación sólido que lo soporte; un currículum vitae, entrevista y un proceso de comprobación de referencias para identificar posibles situaciones que pudieran afectar a la operación del negocio.

Realizar una verificación de sus antecedentes y credenciales.

La corroboración de antecedentes es esencial y debe ser consistente, además de incluir la verificación:

- Empleos anteriores.
- Comprobantes de estudio.
- Antecedentes penales.
- Exámenes toxicológicos.
- Registros de seguridad social y validación.

Establecer controles de acceso apropiados.

Tanto los datos del cliente como los datos internos de la empresa se consideran confidenciales y requieren un especial cuidado cuando se visualizan, almacenan, utilizan, transmiten o eliminan. Es importante definir el rol de cada empleado y establecer un control de acceso a los datos en función de su rol basado en la mejor práctica de **"menor privilegio"**, que permiten al empleado acceder sólo a los datos que son necesarios para realizar su trabajo.

Proporcionar capacitación de seguridad informática los empleados.

Los usuarios directos e indirectos del uso de la tecnología en una empresa son el grupo mas importante de personas que pueden ayudar a reducir los errores involuntarios y las vulnerabilidades de las Tecnologías de la Información.

Por lo que es necesario fomentar una cultura de seguridad informática que les permita comprender las vulnerabilidades de sistemas y las amenazas cibernéticas que pueden estar presentes cuando se usa un equipo de cómputo conectado a la red pública de Internet.

Genere una lista de comprobación de seguridad para los empleados que ya no están laborando en su empresa, independientemente de la razón por la que se van (voluntaria o involuntariamente). Se recomienda asegurarse de que las cuentas de acceso de empleados que finalizaron su relación laboral con la empresa, se borren de inmediato en todos los dispositivos y sistemas informáticos que hayan utilizado.

**Implementar la
lista de verificación
de salida de
empleados.**

Enlaces de ayuda



- "**Curso de Certificación de Contratación Segura en línea**" puede ayudar a sentar las bases para un proceso de reclutamiento seguro.
<http://www.esrcheck.com/ESRonlineSafeHiringCourse.php>
- Para obtener más información sobre las **obligaciones del empleador según la FCRA**, visite <https://mundopymes.org/recursos-humanos/seleccion-de-personal/por-que-verificar-los-antecedentes-generales-de-un-empleado.html>
- "**Kit de concientización** " puede ayudar a sentar las bases para un proceso de concientización
<https://www.incibe.es/protege-tu-empresa/kit-concienciacion>



3.2. Seguridad en dispositivos móviles



Si su empresa utiliza dispositivos móviles para realizar negocios, como acceder al correo electrónico y/o datos confidenciales, preste mucha atención a la seguridad de los dispositivos móviles y las posibles amenazas que pueden poner en peligro sus redes corporativas en general. Esta sección describe el entorno de amenazas móviles y las prácticas que las pequeñas empresas pueden usar para ayudar a proteger dispositivos como teléfonos inteligentes, tabletas y computadoras portátiles conectadas a la red inalámbrica.

Muchas empresas están descubriendo que sus integrantes son más productivos cuando usan dispositivos móviles, y los beneficios son demasiado grandes para ignorarlos. Pero si bien esta tecnología puede aumentar la productividad en el lugar de trabajo, permitir que los empleados traigan sus propios dispositivos móviles a la empresa puede generar importantes desafíos de seguridad y gestión.

- Como la pérdida de datos y su impacto a causa del extravío o el robo de dispositivos electrónicos crean grandes desafíos, ya que éstos se utilizan ahora para almacenar información comercial confidencial y acceder a la red corporativa. Según una encuesta de seguridad móvil de Symantec de diciembre de 2010, el 68 % de los encuestados calificaron la pérdida o el robo como su principal preocupación de seguridad de dispositivos móviles, mientras que el 56 % dijo que los códigos maliciosos para teléfonos móviles es su principal preocupación. Es importante recordar que si bien el empleado puede ser responsable de un dispositivo, la empresa sigue siendo responsable de los datos.



Plan de acción de ciberseguridad

Seguridad en dispositivos móviles

Usar software de seguridad en todos los teléfonos inteligentes.

El software de seguridad, diseñado específicamente para la protección de teléfonos inteligentes, puede detener a los delincuentes informáticos y evitar que roben su información o lo espíen cuando usa redes públicas. Puede detectar y eliminar virus además de otras amenazas móviles antes de que le causen problemas. También puede eliminar mensajes de texto molestos.

Asegurar que todo el software esté actualizado.

Los dispositivos móviles deben tratarse como computadoras personales ya que todo el software de los dispositivos debe mantenerse actualizado, especialmente el que está asociado con la seguridad. Esto protegerá los dispositivos de nuevas variantes de códigos maliciosos que amenazan la información crítica de su empresa.

Asegurar que todos los dispositivos no cuenten con información antes de su eliminación.

La mayoría de los dispositivos móviles tienen una función de reinicio que permite borrar todos los datos. Las tarjetas SIM también deben eliminarse y destruirse.

La información empresarial y personal almacenada en dispositivos móviles a menudo es delicada. Cifrar esta información es otra obligación. Si se pierde un dispositivo y se roban la tarjeta SIM, no se podrá acceder a los datos si se aplica la tecnología de cifrado adecuada en el dispositivo.

Cifrar los datos en dispositivos móviles.

Además de aplicar las actualizaciones de seguridad e implementar cifrado en los dispositivos móviles, es importante utilizar contraseñas seguras para proteger los datos almacenados. Esto contribuirá en gran medida a evitar que una persona no autorizada acceda a datos confidenciales si el dispositivo se pierde o lo roban.

Hacer que usuarios protejan con contraseña el acceso a los dispositivos móviles.

En el caso de una pérdida o robo, los empleados y la gerencia deberían saber qué protocolo aplicar. Deben existir procesos para desactivar el dispositivo y proteger su información de la intrusión.

Establecer un procedimiento de denuncia para equipos y datos perdidos o robados.

Enlaces de ayuda



- Enseñe a sus empleados sobre aplicaciones móviles:
<http://onguardonline.gov/articles/0018-understanding-mobile-apps>
- Mantenga sus computadoras portátiles seguras:
<http://onguardonline.gov/articles/0015-laptop-security>
- "Guía para el Borrado Seguro de Datos Personales" puede ayudar a sentar las bases para el desarrollo de un guía:
http://inicio.ifai.org.mx/DocumentosdelInteres/Guia_Borrado_Seguro_DP.pdf



3.3. Seguridad en la Red



Asegurar la red de su compañía consiste en:

- Identificar todos los dispositivos y conexiones en la red.
- Establecer límites entre los sistemas de su compañía y otros.
- Hacer cumplir los controles para garantizar que en caso de que ocurra un acceso no autorizado, uso indebido o cualquier evento de negación de servicio puedan frustrarse, contenerse y recuperarse rápidamente.



Plan de acción de ciberseguridad

Seguridad en la Red

Actualizar regularmente todas las aplicaciones.

Todos los equipos de cómputo, aplicaciones y software, incluido el equipo de red, deben actualizarse de manera oportuna a medida que estén disponibles. Utilice servicios de actualización automática siempre que sea posible, especialmente para sistemas de seguridad como aplicaciones antivirus, herramientas de filtrado web y sistemas de prevención de intrusiones.

Establecer reglas seguras de navegación web.

La red interna de su empresa únicamente debe acceder a los servicios y recursos en Internet que son esenciales para el negocio y las necesidades de sus empleados. Utilice las características de navegación segura incluidas en los navegadores web o herramientas específicas para garantizar que no se pueda acceder a sitios maliciosos o no autorizados desde su red corporativa.

Si el acceso remoto está habilitado, verificar que sea seguro.

Si la compañía necesita proporcionar acceso remoto a su red corporativa a través de Internet, una opción común y segura es emplear un sistema de Red Privada Virtual (VPN), se recomienda que esta medida esté acompañada de la buena práctica de doble autenticación.

Crear una política de unidad flash de uso seguro.

Asegúrese de que los empleados nunca coloquen algún dispositivo de almacenamiento externo desconocido (USB, disco externo, entre otros) en su computadora. Las pequeñas empresas deben establecer una política para que los empleados sepan que nunca deben abrir un archivo desde una unidad externa con la que no están familiarizados.

Asegurar la red inalámbrica (Wi-Fi) de su empresa.

Control de Acceso Inalámbrico: Separar la red principal de la empresa, optar por una red local inalámbrica (WLAN) para el uso de clientes, invitados y visitantes. Todos los usuarios deben recibir credenciales únicas con fechas de caducidad preestablecidas para poder acceder a la WLAN.

Cifrado de la red inalámbrica: Se recomienda que la WLAN de su empresa utilice el nivel de cifrado Wi-Fi Protected Access 2 (WPA2).

Proteger los datos que la empresa considere como confidenciales y que estén tanto en disco como en transmisión por una red inalámbrica. Además de cumplir los requisitos normativos aplicables sobre protección de la información. Aunado a lo anterior, se recomienda utilizar protocolos de cifrado SSL para los sitios web de la empresa que realicen autenticaciones en línea.

Emplear contraseñas más fuertes con factor de doble autenticación. Además de alentar a sus empleados a emplear contraseñas complejas que cumplan con las características mínimas de seguridad.

La red de producción debe estar separada de la red pública de Internet, con mecanismos de seguridad perimetrales que autenticuen usuarios y sistemas de la red interna, tales como firewalls y servidores proxy de filtrado web.

Red interna

Identificar los límites de red de su empresa y evaluar el tipo de control necesario, Configurar los dispositivos fronterizos sólo para permitir conexiones hacia y desde las direcciones IP públicas de su empresa, implementar protecciones de firewalls en el perímetro de su red para restringir peticiones únicamente hacia servicios necesarios y configurar sistemas de prevención de intrusos para supervisar actividades sospechosas dentro de la red.

Servicios en la nube

Consultar términos y condiciones de su proveedor de servicios en la nube, asegurarse que la información y actividades estén protegidas, solicite seguridad y auditorías según las necesidades de su empresa y revise los acuerdos de nivel de servicio además de consultar servicios adicionales como respaldos de información y cifrado.

Cifrar datos sensibles de la compañía.

Establecer políticas de contraseñas seguras.

Asegurar la red interna y servicios en la nube.



Enlaces de ayuda

- Para obtener más información visite:
<https://www.uschamber.com/CybersecurityEssentials>
- Para obtener más información visite:
www.clavessegura.org

3.4. Prevención de fraude electrónico



Las nuevas tecnologías de información y telecomunicaciones pueden ofrecer innumerables oportunidades para las pequeñas empresas, pero también ofrecen a los ciberdelincuentes muchas nuevas formas de victimizar a su negocio y mediante algún tipo de fraude a los clientes dañar su reputación y a sus clientes. Las empresas de todos los tamaños deben conocer los fraudes más comunes que se cometen en línea.

Para proteger su empresa contra fraudes en línea, tenga cuidado al visitar enlaces web o abrir archivos adjuntos de remitentes desconocidos, asegúrese de mantener todo el software actualizado y monitoree constantemente las cuentas bancarias para detectar actividades no autorizadas.



Plan de acción de ciberseguridad

Prevención de estafas y fraude electrónico

Capacitar a los empleados para reconocer la ingeniería social.

La ingeniería social, es una técnica de engaño utilizada por muchos delincuentes, tanto en línea como fuera de ella, para obtener información personal o comercial y / o instalen software malicioso en sus computadoras, dispositivos o redes.

La mayoría de la ingeniería social fuera de línea ocurre por teléfono, pero también ocurre con frecuencia en línea. La información recopilada de las redes sociales o publicada en sitios web puede ser suficiente para crear una artimaña convincente y engañar a sus empleados.

Protegerse contra el fraude en línea.

El fraude en línea adopta muchas formas que pueden afectar a todos, incluidas las pequeñas empresas y sus empleados.

Asegúrese de nunca solicitar información personal o datos confidenciales a través de correo electrónico, redes sociales u otros mensajes en línea. Hágales saber a sus clientes que su empresa nunca solicitará este tipo de información a través de dichos canales y solicíteles que se comuniquen con usted directamente si tienen alguna inquietud o sospecha.

Protegerse contra el malware.

Muchas empresas están siendo víctimas del malware para registrar las pulsaciones de teclas hechas en la computadora infectada, lo que permite a los delincuentes ver contraseñas, números de tarjetas de crédito y otros datos personales, se recomienda que los dispositivos electrónicos cuenten con un software antimalware, el cual permitirá detectar y eliminar amenazas maliciosas.

Protegerse contra el phishing.

El phishing es la técnica de ingeniería social utilizada por los delincuentes para engañar a las personas y hacerles creer que están visitando el sitio web de su confianza.

Esta técnica es usada para aprovecharse de los clientes y empleados desprevenidos, para robar sus credenciales de acceso y números de tarjetas de crédito.

Si cree que ha revelado información confidencial sobre su organización, asegúrese de:

- Informar del incidente a las personas apropiadas dentro de su organización, de acuerdo a la normatividad.
- Comuníquese con su institución financiera y cierre cualquier cuenta que pueda haber sido comprometida (si considera que los datos financieros están en riesgo).
- Cambie las contraseñas que haya revelado y, si utilizó la misma contraseña para varios recursos, asegúrese de cambiarla para cada cuenta.

Clientes:

- Nunca solicitar a sus clientes que envíen información sensible por correo electrónico, visitas personales o por teléfono.
- Hacer una campaña de concientización que refuerce que nunca solicitará información personal por correo electrónico, de modo que si alguien apunta a sus clientes, es posible que se den cuenta que la solicitud es un fraude.
- Realizar los avisos de privacidad correspondientes y realizar su difusión en toda la empresa.

Empleados:

- La conciencia de los empleados es su mejor defensa contra los usuarios engañados para que entreguen sus nombres de usuario y contraseñas a los delincuentes cibernéticos.
- Nunca deben responder a los mensajes entrantes que solicitan información o datos personales.
- Verificar la identidad con la compañía que se indica antes de compartir cualquier información personal o clasificada.
- Nunca deben abrir un enlace enviado por correo electrónico desde una fuente no confiable.



Plan de acción de ciberseguridad

Seguridad en la Red

No se deje engañar por las falsas ofertas de antivirus.

Los falsos antivirus y otros programas fraudulentos en línea han estado detrás de algunos de los delitos en línea más exitosos en los últimos tiempos.

- Asegúrese de que su organización cuente con una política que explique cuál es el procedimiento si la computadora de un empleado se infecta con un virus informático.
- Capacite a sus empleados para reconocer un mensaje de advertencia legítimo.
- Configure sus computadoras para que no permitan que los usuarios sin privilegios tengan acceso administrativo para instalar cualquier otro tipo de software.

Crear una estrategia de seguridad en capas contra software malicioso.

El software antivirus es recomendable, pero no debe ser la única línea de defensa de una empresa. En su lugar, implemente una combinación de muchas técnicas para mantener su entorno seguro.

- Uso de filtrado web .
- Protección con motores antivirus.
- Firewalls.
- Políticas de seguridad sólidas.
- Capacitación de los empleados.
- Software actualizado.

Verificar la identidad de las personas que hablan a la empresa solicitando información.

Asegúrese de capacitar a los empleados para que nunca revelen información del cliente o de la empresa, nombres de usuario, contraseñas u otros detalles confidenciales a las personas que llaman. Siempre verificar la identidad y la validez de la persona y su solicitud.

Enlaces de ayuda



- Para obtener más información visite:
<http://www.eicar.org/>

3.5. Privacidad y seguridad de datos



La seguridad de los datos es crucial para todas las pequeñas empresas. Información de los empleados, clientes, información de pago, archivos personales y detalles de la cuenta bancaria: toda esta información a menudo es imposible de reemplazar si se pierde además de ser peligrosa en manos de delincuentes. La pérdida de datos debido a desastres como una inundación o un incendio es devastadora, pero perderla a causa de ciberdelincuentes o por una infección de malware puede tener consecuencias mucho mayores. La forma en cómo maneja y protege sus datos es fundamental para la seguridad de su negocio y las expectativas de privacidad de los clientes, empleados y socios.



Plan de acción de ciberseguridad

Privacidad y seguridad de datos

Realizar un inventario de activos de información.

Contestando las siguientes preguntas:

¿Qué tipo de información tienes en tu negocio?

Una empresa típica tiene todo tipo de datos, algunos de ellos más valiosos y sensibles que otros, pero todos los datos tienen valor para alguien.

¿Cómo se manejan y protegen esos datos?

Como propietario de una pequeña empresa, debe tener un plan y una política (un conjunto de pautas, si lo desea) sobre cómo se debe manejar, validar y proteger cada tipo de datos en función de dónde viaja y quién lo utilizará.

¿Quién tiene acceso a esa información y en qué circunstancias?

No todos los empleados necesitan acceso a toda su información. Su personal de marketing no debería necesitar ni tener permiso para ver los datos de nómina de los empleados, y es posible que su personal administrativo no necesite acceder a toda su información de cliente.

Desarrollar una política de privacidad.

La privacidad es importante para su negocio y sus clientes. La confianza continua en sus prácticas comerciales, productos y manejo seguro de la información única de sus clientes afecta su rentabilidad. Su política de privacidad es una promesa a sus clientes de que usará y protegerá su información de la forma que ellos esperan y que cumplan con sus obligaciones legales.

Su política de privacidad deberá abordar los siguientes tipos de datos:

- Información de identificación personal.
- Información de salud personal.
- Información del cliente.

Su sitio web puede ser un excelente lugar para recopilar información, desde transacciones y pagos hasta el historial de compras y navegación, e incluso registros de boletines informativos, consultas en línea y solicitudes de clientes. Debe asegurarse de que los datos recopilados a través de su sitio web y los que son almacenados por un tercero sean lo suficientemente seguros.

Proteger datos recopilados en internet.

Cada empresa debe planificar lo inesperado, y eso incluye la pérdida o el robo de datos de su empresa. La pérdida o el robo de datos no sólo puede dañar su negocio, marca y confianza del cliente, sino que también debe observar las regulaciones estatales y federales a menudo son muy costosas las que cubren la protección de datos y la privacidad.

Establecer un plan para pérdida o robo de datos.

La idea de la seguridad en capas es simple: no puede y no debe confiar en un sólo mecanismo de seguridad, como una contraseña, para proteger algo sensible. Si ese mecanismo de seguridad falla, no le quedará nada para protegerlo.

Cuando se trata de seguridad de datos, hay una serie de capas técnicas y de procedimientos clave en materia de ciberseguridad que debe considerar:

Crear una estrategia de seguridad en capas.

- Inventario de sus datos.
- Identificar y proteger los datos sensibles y valiosos (Ultra confidencial, secreta y uso interno).
- Controlar el acceso a sus datos (Cuanto más sensibles sean los datos, más restrictivo será el acceso).
- Asegurar sus datos.
- Revisar que las disposiciones legales en materia de privacidad y protección de datos personales se adecuen a los procedimientos técnicos de seguridad de la información.

Enlaces de ayuda

- Para obtener más información visite:
<http://www.bbbonline.org/reliability/privacy/>





3.6. Seguridad en los sistemas informáticos y Sitios Web



Los servidores web, que alojan los datos y otro contenido disponible para sus clientes en Internet, a menudo son los componentes más expuestos y atacados de la red de una empresa. Los ciberdelincuentes están constantemente buscando sitios web poco seguros para atacar, mientras que muchos clientes dicen que la seguridad del sitio web es una consideración importante cuando eligen comprar en línea. Como resultado, es esencial proteger los servidores y la infraestructura de red que los respalda. Las consecuencias de una violación de seguridad son grandes: pérdida de

Ejemplos de amenazas de seguridad específicas para servidores web:

- **Explotar errores de software y programación en el servidor web**, a través del sistema operativo subyacente o el contenido activo se puede obtener acceso no autorizado al servidor web.
- **Denegación de servicio**, pueden dirigirse al servidor web o a su infraestructura de red de soporte para evitar u obstaculizar que los usuarios de su sitio web utilicen sus servicios.



Plan de acción de ciberseguridad

Seguridad en los sistemas informáticos y Sitios Web

Establecer roles de seguridad y responsabilidades.

Uno de los medios más efectivos y menos costosos para prevenir incidentes graves de ciberseguridad es establecer una política que defina claramente la separación de roles y responsabilidades con respecto a los sistemas y la información que contienen. Muchos sistemas están diseñados para proporcionar un fuerte Control de Acceso Basado en Roles (RBAC), pero esta herramienta es de poca utilidad sin procedimientos y políticas de seguridad bien definidos que rijan la asignación de roles y sus limitaciones asociadas.

Dichas políticas deben establecer claramente, como mínimo:

- Los roles necesarios, y los privilegios y restricciones acordados a esos roles.
- Los tipos de empleados a los que se les debe permitir asumir los diversos roles
- Cuánto tiempo un empleado puede tener un rol.
- Si los empleados pueden tener múltiples roles, las circunstancias que definen cuándo adoptar un rol sobre otro.

Identificar posibles riesgos de reputación.

Todas las empresas deben tomarse el tiempo para identificar los riesgos potenciales para su reputación y desarrollar una estrategia para mitigar esos riesgos a través de políticas u otras medidas disponibles.

Enlaces de ayuda



- Para obtener más información visite:
http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472018000100267

3.7. Seguridad en servicios de correo electrónico



El correo electrónico se ha convertido en una parte fundamental de nuestro negocio cotidiano, desde la administración interna hasta la atención directa al cliente. Los beneficios asociados con el uso de correo electrónico como una herramienta comercial primaria superan ampliamente los aspectos negativos. Sin embargo, las empresas deben tener en cuenta que una plataforma de correo electrónico exitosa comienza con los principios básicos de la seguridad del correo electrónico para garantizar la privacidad y la protección de la información del cliente y del negocio.



Plan de acción de ciberseguridad

Seguridad en servicios de correo electrónico

Configurar un filtro de correo electrónico no deseado.

Está bien documentado que el spam, los intentos de phishing y el correo electrónico no solicitado o no deseado a menudo representan más del 60 % de todos los correos electrónicos que recibe una persona o empresa. El correo electrónico es el principal medio para propagar virus y malware, y es uno de los más fáciles de defender.

Considere:

- Filtro de correo electrónico.
- Asegúrese de que las actualizaciones automáticas estén habilitadas.
- Asegúrese de que los filtros se revisen regularmente para que el correo electrónico o los dominios importantes no se bloqueen por error.

Capacite a sus empleados en el uso responsable del correo electrónico.

Los empleados deben estar capacitados para identificar los riesgos asociados con el uso del correo electrónico, cómo y cuándo usar un correo electrónico apropiado para su trabajo y cuándo buscar ayuda de profesionales. La capacitación de concientización de empleados está disponible en muchas formas, incluidos medios impresos, videos y capacitación en línea.

Proteger la información confidencial enviada por correo electrónico.

Con su proliferación como una herramienta principal para comunicarse interna y externamente, el correo electrónico comercial a menudo incluye información confidencial. Ya sea información de la compañía que pueda dañar su negocio o datos regulados como la información personal, es importante asegurarse que ésta sólo sea enviada y consultada por quienes tienen derecho a verla.

Establecer una política de almacenamiento de correo sensible.

Desde el costo de almacenamiento y respaldo, hasta los requisitos legales y regulatorios, las empresas deben documentar cómo manejarán el tiempo de almacenamiento del correo electrónico e implementarán controles básicos para aplicar las políticas.

Muchas empresas tienen reglas específicas que dictan cuánto tiempo pueden o deben almacenar los correos electrónicos. Muchas implementan un estándar de almacenamiento de 60-90 días si no están obligados por ley a otro período de retención.

Las políticas son importantes para establecer expectativas con sus empleados o usuarios, y para desarrollar estándares que garanticen el cumplimiento de sus políticas publicadas.

Sus políticas deben ser fáciles de leer, comprender, definir y hacer cumplir. Otras áreas de políticas deben abordar el almacenamiento, la privacidad y el uso aceptable.

Desarrollar una política de uso de correo electrónico.

Enlaces de ayuda



- Para obtener más información visite:
http://www.sans.org/security-resources/policies/Email_Policy.pdf

3.8. Políticas de seguridad



Todas las empresas deben desarrollar y mantener políticas claras y sólidas para salvaguardar datos críticos de la empresa e información sensible, proteger su reputación y evitar el comportamiento inapropiado de los empleados.

Muchos de estos tipos de políticas ya existen para situaciones del "mundo real", pero pueden necesitar adaptarse a su organización y actualizarse para reflejar el impacto creciente del ciberespacio en las transacciones cotidianas, tanto profesionales como personales. Al igual que con cualquier otro documento de la organización, las políticas de seguridad cibernética deben seguir buenas prácticas de diseño y gobernanza, evitando que se vuelvan inutilizables y sean revisadas periódicamente para garantizar que sigan siendo pertinentes a medida que su empresa cambia.

Recuerde que para mayor resultados dentro de la implementación y desarrollo de sus políticas debe abordar todos los requisitos como las leyes federales, estatales o locales.



Plan de acción de ciberseguridad

Políticas de seguridad

Establecer una política de uso de Internet para los empleados.

Los límites en el uso de Internet de los empleados en el lugar de trabajo varían ampliamente de una empresa a otra. Sus pautas deben permitirles a los empleados el máximo grado de libertad que requieren para ser productivos (se ha demostrado que los descansos cortos para navegar por Internet o realizar tareas personales en línea aumentan la productividad). Al mismo tiempo, las reglas de comportamiento son necesarias para garantizar que todos los empleados conozcan los límites, tanto para mantenerlos seguros como para mantener su empresa.

- Si utiliza un sistema de filtrado web, los empleados deben tener un conocimiento claro de cómo y por qué se controlarán sus actividades web, además de qué tipos de sitios son considerados no permitidos por su política.
- Los descansos personales para navegar por la web deben limitarse a un período razonable y a ciertos tipos de actividades.

Una política de medios sociales sólida es crucial para cualquier empresa que busque utilizar las redes sociales para promover sus actividades y comunicarse con sus clientes. Como mínimo, una política de redes sociales debe incluir claramente lo siguiente:

- Orientación específica sobre cuándo divulgar las actividades de la empresa a través de las redes sociales y qué tipo de detalles se pueden discutir en un foro público.
- Reglas de comportamiento adicionales para los empleados que usan cuentas personales de redes sociales para aclarar qué tipos de temas o publicaciones de discusión podrían generar riesgos para la compañía.
- Asesoría sobre el uso de la dirección de correo electrónico de la empresa en sitios web públicos.
- Orientación sobre la selección de contraseñas largas y seguras para cuentas de redes sociales.

***Establecer una
política de redes
sociales.***

Enlaces de ayuda



- Para obtener más información visite::
<http://www.cert.org/governance/>

3.9. Respuesta a incidentes de seguridad



Aún con estructuras y planes de seguridad cibernética bien implementados, no se pueden evitar violaciones a los mecanismos de seguridad que resguardan los datos de su empresa, por lo que debe asegurarse de contar con procedimientos para responder a dichas violaciones de seguridad cuando ocurran.

Tipos de incidentes:

- **Incidentes físicos:** incluyen incidentes del mundo real, como robos y extravío de equipos, así como cualquier evento en el que los equipos de su empresa se vean afectados.
- **Incidentes de seguridad de red:** incluyen eventos cuando las computadoras se infectan con código malicioso, personas no autorizadas acceden a ellas de forma remota o son utilizadas por personas autorizadas para realizar alguna actividad maliciosa.
- **Incidentes de exposición de datos,** es decir, la fuga o la divulgación de información sensible en canales inseguros, pueden ser el resultado de cualquiera de los tipos de eventos descritos anteriormente.



Plan de acción de ciberseguridad

Respuesta a incidentes de seguridad

Notificar a la policía si es necesario.

Según el tipo de infracción y el tipo de negocio, es posible que su empresa deba notificar a la Unidad Cibernética de la Guardia Nacional, autoridad local u otras autoridades gubernamentales al descubrir una violación a la seguridad informática de su organización. En caso de exposición de la información del cliente, debe notificar al cliente (s) del incidente, registrar los datos que se perdieron o quedaron expuestos y registrar las medidas tomadas para asegurar una exposición futura.

Trabajar coherentemente entre los equipos técnicos y los directivos para minimizar el daño.

Una vez que su empresa se da cuenta de que se ha producido un incidente de seguridad, el personal técnico y los responsables de la toma de decisiones empresariales deben trabajar juntos para decidir cuál es el plan de contención más práctico y efectivo. Los planes de contención variarán de un conjunto de circunstancias a otro, y pueden convertirse rápidamente en intensivos en términos de tiempo y recursos desde las perspectivas de impacto tecnológico y comercial.

En cualquier caso, la contención de los incidentes cibernéticos debe centrarse en determinar el alcance del compromiso y preservar la confidencialidad e integridad de los datos sensibles que aún no han sido robados o divulgados.

Otros aspectos que afectan la selección y ejecución de un plan de contención incluyen la estrategia de gestión de riesgo y reputación de su compañía y la decisión de solicitar asistencia externa, ya sea de las entidades locales o federales, una firma consultora privada o una organización de respuesta a incidentes informáticos.

Después de que se haya establecido un plan de contención y haya comenzado su ejecución, comience con los esfuerzos de erradicación y recuperación. En el caso de vulneraciones de seguridad de la red y de los sistemas, la erradicación generalmente significa eliminar todos los rastros de software no autorizado de la red y deshabilitar todos los privilegios de acceso asociados con las cuentas de usuario que han sido parte de la actividad maliciosa.

Principios clave de recuperación de desastres:

- No espere hasta que sea demasiado tarde.
- Proteja la información por completo.
- Involucre a los empleados.
- Realice simulacros de crisis frecuentemente.
- Revise su plan.
- Esté preparado.

Por último, su empresa siempre debe realizar una reunión de "lecciones aprendidas" después de que la fase de recuperación se haya completado con éxito para descubrir, documentar y refinar el conocimiento adquirido durante el proceso de manejo de incidentes. Es importante involucrar a las áreas jurídicas y de la alta dirección en estas reuniones.

***Comience el
esfuerzo de
recuperación.***

***Realizar una
reunión de
"lecciones
aprendidas".***



Enlaces de ayuda

- Para obtener más información visite:
[*Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales.*](#)

3.10. Seguridad de las operaciones



En un contexto comercial, la seguridad de las operaciones (“OPSEC” por sus siglas en inglés) es el proceso de negar a los ciberdelincuentes el acceso a cualquier información de la empresa a través de la planificación y ejecución de actividades que son esenciales para el éxito de las operaciones.

Consta de cinco acciones distintas:

- Identifique la información que es crítica para su negocio.
- Analice la amenaza a esa información crítica.
- Analice las vulnerabilidades de su empresa que permitirían a un delincuente cibernético tener acceso a información.
- Evalúe el riesgo para su negocio si las vulnerabilidades son explotadas satisfactoriamente.
- Aplicar contramedidas para mitigar los factores de riesgo.



Plan de acción de ciberseguridad

Seguridad de las operaciones

Identidad de la información crítica.

Proteger la información crítica o vital en lugar de intentar proteger toda la información de las operaciones de la organización. Dado que cualquier empresa tiene tiempo, personal y dinero limitados para desarrollar prácticas comerciales seguras, es esencial enfocar esos recursos limitados en la protección de la información que es más importante para las operaciones críticas. Algunos ejemplos de información crítica incluyen lo siguiente:

- Listas de clientes e información de contacto.
- Contratos.
- Patentes y propiedad intelectual.
- Arrendamientos y escrituras.
- Manuales de políticas y proceso.
- Documentos corporativos.
- Planes estratégicos y minutas de reuniones de la dirección.

Es importante destacar que lo que es información crítica para una empresa puede no ser crítica para otra. Utilice la misión de su empresa como una guía para determinar qué datos son realmente vitales.

Analizar las amenazas.

Esta acción implica la investigación y el análisis para identificar posibles delincuentes cibernéticos que pueden intentar obtener información crítica de las operaciones de su empresa. Los indicadores de seguridad de las operaciones en su empresa deben responder las siguientes preguntas de información crítica:

- ¿Quién podría ser un ciberdelincuente (por ejemplo, competidores, intrusos informáticos con motivaciones políticas, etc.)?
- ¿Cuáles son los objetivos del ciberdelincuente?
- ¿Qué acciones podría tomar el delincuente cibernético?
- ¿Qué información crítica tiene el cibercriminal de las operaciones de su empresa? (es decir, ¿qué información está ya disponible públicamente?)

El objetivo de esta acción es identificar las vulnerabilidades de su empresa para proteger la información crítica. Requiere examinar cada aspecto de la seguridad que busca proteger su información crítica y luego comparar esos indicadores con las amenazas identificadas en el paso anterior.

Las vulnerabilidades comunes para las pequeñas empresas incluyen las siguientes:

- Dispositivos móviles con poca seguridad que tienen acceso a información crítica.
- Falta de política sobre qué información y equipo en red se pueden llevar a casa o llevarse a viajes de negocios al extranjero.
- Almacenamiento de información crítica en cuentas de correo electrónico personales u otras redes que no pertenecen a la compañía.
- Falta de política sobre qué información de la empresa puede ser publicada o accedida por sitios de redes sociales.

Esta acción tiene dos componentes:

1. En primer lugar, los gerentes de seguridad de las operaciones deben analizar las vulnerabilidades identificadas en la acción anterior e identificar las posibles medidas para mitigar cada una.
2. En segundo lugar, las medidas específicas de seguridad de las operaciones deben seleccionarse para su ejecución en función de una evaluación de riesgos realizada por el personal directivo de su empresa.

La evaluación de riesgos requiere comparar el costo estimado asociado con la implementación de cada posible medida de seguridad de las operaciones con los posibles efectos perjudiciales en las operaciones de la empresa como resultado de la explotación de una vulnerabilidad particular.

Analice las vulnerabilidades.

Evaluar el riesgo.



Plan de acción de ciberseguridad

Seguridad de las operaciones

Las medidas pueden implicar algún costo en tiempo, recursos, personal o interferencia con las operaciones cotidianas. Si el costo para lograr su protección excede el costo del daño que un atacante podría infligir, entonces la aplicación de la medida es inapropiada. Debido a que la decisión de no implementar una medida de seguridad de las operaciones particular conlleva riesgos, este paso requiere la aprobación de la presidencia de su empresa.

Aplicar medidas apropiadas de seguridad de las operaciones .

En esta acción, la dirección de su empresa revisa e implementa las medidas de seguridad de las operaciones seleccionadas en la evaluación de la acción de riesgo. Antes de poder seleccionar las medidas, se deben conocer los objetivos de seguridad y la información crítica, identificar los indicadores y evaluar las vulnerabilidades.



Enlaces de ayuda

- Para obtener más información visite:
<http://www.opsecprofessionals.org/>

3.11. Seguridad en mecanismos de pago electrónico



Si su empresa acepta pagos con tarjetas de crédito o débito, es importante contar con medidas de seguridad para garantizar la seguridad de la información de sus clientes. También puede tener obligaciones de seguridad según los acuerdos con su banco o procesador de servicios de pago. Estas entidades pueden ayudarlo a prevenir fraudes. Además, hay recursos gratuitos y consejos generales de seguridad disponibles para aprender cómo mantener segura la información sensible, más allá de la información de pago.



Plan de acción de ciberseguridad

Seguridad de las operaciones

Realice un directorio con los datos de clientes y sus tarjetas.

Haga una lista del tipo de información de clientes y tarjetas que recopila y guarda: nombres, direcciones, información de identificación, números de tarjetas de pago, datos de banda magnética, detalles de cuentas bancarias y números de Seguridad Social. No son sólo los números de tarjeta lo que los criminales quieren; están buscando todo tipo de información personal, especialmente si les ayuda a cometer un robo de identidad:

- Es importante tener presente dónde guarda esa información y cómo está protegida.
- Determine quién tiene acceso a estos datos y si necesitan tener acceso.
- Realice los avisos de privacidad conducentes.

Evalúa si necesitas conservar todos los datos que almacenas.

Una vez que sepa qué información recopila y almacena, evalúe si realmente necesita conservarla. A menudo las empresas pueden no darse cuenta de qué están registrando o de lo contrario mantienen datos innecesarios hasta que realizan una auditoría.

Si ha estado usando números de tarjeta para fines distintos a las transacciones de pago, como un programa para identificar más rápido a sus clientes, pregúntele a su procesador financiero si puede utilizar datos alternativos. El uso de tokens, por ejemplo, es una tecnología que enmascara los números de tarjeta y la reemplaza con un número alternativo que no puede usarse para el fraude.

Use herramientas y servicios seguros.

- La industria de pagos mantiene listas de hardware, software y proveedores de servicios que han sido validados contra los requisitos de seguridad de la industria.
- Las pequeñas empresas que utilizan sistemas de pago integrados, en los que el terminal de la tarjeta está conectado a un sistema informático más grande, pueden consultar la lista de aplicaciones de pago validadas para asegurarse de que se haya probado el software que emplean.

- Ya sea que use un sistema de pago más complicado o un terminal independiente simple, asegúrese cuidadosamente controlar el acceso.
- Aislar los sistemas de pago de otros programas menos seguros, especialmente aquellos conectados a Internet. Por ejemplo, no use la misma computadora para procesar pagos y navegar por Internet.
- Controle o limite el acceso a los sistemas de pago sólo a los empleados que necesitan acceso.
- Asegúrese de utilizar un sistema seguro para acceso remoto o elimine el acceso remoto si no lo necesita para que los delincuentes no puedan infiltrarse en su sistema desde

***Controlar el
acceso a los
sistemas de
pago.***

Trabaje con su banco o proveedor financiero y pregunte acerca de las medidas, herramientas y servicios contra el fraude que puede utilizar para garantizar que los delincuentes no puedan usar la información de la tarjeta robada en su negocio.

Para los minoristas de comercio electrónico:

- El código CVV2 es el número de tres dígitos en el panel de firma que puede ayudar a verificar que el cliente tenga posesión física de la tarjeta y no sólo el número de cuenta.
- Los minoristas también pueden usar el Servicio de verificación de direcciones para asegurarse de que el titular de la tarjeta proporcionó la dirección de facturación correcta asociada con la cuenta.
- Los servicios como Verified by Visa solicitan al titular de la tarjeta que ingrese una contraseña personal que confirma su identidad y proporciona una capa adicional de protección.

***Use
herramientas
y recursos de
seguridad.***

**Use
herramientas y
recursos de
seguridad.**

**Recuerda los
principios básicos
de seguridad.**

Para los minoristas :

- Pase la tarjeta y obtenga una autorización electrónica para la transacción.
- Verifique que la firma coincida con la tarjeta.
- Asegúrese de que su terminal de pago esté seguro y protegido contra manipulaciones.
- Use contraseñas fuertes y únicas y cámbielas con frecuencia.
- Utilice las últimas tecnologías de firewall y antivirus.
- No haga clic en enlaces sospechosos que pueda recibir por correo electrónico o en línea.



Enlaces de ayuda

- Te recomendamos consultar el siguiente documento:
https://www.pcisecuritystandards.org/pdfs/pci_dss_spanish.pdf
- Visa ofrece una guía de seguridad de datos para pequeñas empresas como parte de su Programa de seguridad de la información del titular de la tarjeta:
<http://usa.visa.com/download/merchants/uscc-cyber-security-guide-2012.pdf>
- La información sobre los estándares de seguridad de la industria está disponible en el PCI Security Standards Council:
<https://www.pcisecuritystandards.org>

3.12. Seguridad física



Proteger a los empleados y miembros del público que visitan sus instalaciones es una responsabilidad compleja y desafiante. También es una de las principales prioridades de su empresa.



Plan de acción de ciberseguridad

Seguridad física

Reconozca la importancia de asegurar las instalaciones de la empresa.

Es fácil pensar en la seguridad física de la empresa como un mero ejercicio para mantener el control de los puntos de acceso y garantizar la total visibilidad en las áreas que se consideran de alto riesgo, ya sea por la amenaza de un fácil acceso público o por el valor de la información que se encuentra cerca. Sin embargo, mantener la seguridad de las instalaciones de su empresa también incluye el entorno físico de los espacios públicos. Por ejemplo:

- Los empleados cuyas computadoras tienen acceso a información confidencial no deben tener sus monitores de la computadora dirigidos hacia espacios de acceso público como áreas de recepción, mostradores de facturación y salas de espera.
- Las computadoras portátiles, tabletas electrónicas y teléfonos celulares, deben ubicarse lejos de las áreas públicas.
- En los casos en que se almacena información extremadamente confidencial en una computadora portátil, considere agregar un sistema de software LoJack.
- Minimice y proteja los materiales impresos con información sensible.
- Considere la implementación de un sistema de identificación de distintivos para todos los empleados, y capacite a los empleados para detener e interrogar a cualquier persona en el área comercial operativa sin una insignia o que parezca ser un visitante sin escolta.

Capacite a sus empleados en los procedimientos de seguridad de la instalación.

Una violación de la seguridad de la información del cliente o una violación de la información interna de la empresa puede resultar en una pérdida de confianza pública y puede ser tan devastador para su como un desastre natural. Para abordar tales riesgos, debe dedicar su tiempo, atención y recursos (incluido el tiempo de capacitación de los empleados) a las vulnerabilidades potenciales en su entorno comercial y los procedimientos y prácticas que deben ser una parte estándar del día de trabajo de cada empleado.

Con demasiada frecuencia, la información confidencial, incluida la información de identificación personal de los clientes, información financiera y de otro tipo, y la información de acceso al sistema de la compañía, está disponible para que la encuentren en la basura.

- Invierta en trituradoras.
 - Contrate a una compañía de trituración de confianza.
 - Desarrolle procedimientos estándar y programas de capacitación para empleados a fin de garantizar que todos en su empresa conozcan qué tipo de información se debe triturar.
-
- Tenga en cuenta que vaciar la papelera de reciclaje en su escritorio o eliminar documentos de las carpetas de su computadora u otro dispositivo electrónico puede no eliminar la información para siempre. Aquellos con habilidades informáticas avanzadas aún pueden acceder a su información, incluso después de que crea que la ha destruido.

***Eliminar la basura
de forma segura.***

***Deseche el equipo
electrónico de
forma segura.***

Enlaces de ayuda



- Consejos de seguridad física para tu PyME
<https://www.impulsapopular.com/gerencia/consejos-de-seguridad-fisica-para-tu-pyme/>

Glosario

Amenaza:

Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor.

Cloud computing:

Permite a los usuarios almacenar información, ficheros y datos en servidores de terceros, de forma que puedan ser accesibles desde cualquier terminal con acceso a la nube o a la red, resultando de esta manera innecesaria la instalación de software adicional (al que facilita el acceso a la red) en el equipo local del usuario.

Cifrado:

Es un procedimiento que utiliza un algoritmo para codificar los datos con cierta clave, de tal forma que dejan de estar en su con cierta clave para transformar un mensaje formato original por lo que no se pueden leer, es decir son incomprensibles o al menos difícil de comprender a toda persona que no tenga la clave del algoritmo.

Comercio electrónico:

Es el desarrollo de operaciones comerciales a través de internet, tales como el proceso de compra, venta o intercambio de bienes, servicios e información a través de la redes de comunicación.

CONDUSEF: Es la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, la cual promueve y difunde la educación y la transparencia financiera para que los usuarios tomen decisiones informadas sobre los beneficios, costos y riesgos de los productos y servicios ofertados en el sistema financiero mexicano.

Criptomoneda:

Es una moneda virtual que se crea y se almacena electrónicamente, no está regulada por ningún tipo de gobierno, el precio de una moneda virtual se determina por la oferta y la demanda.

Denegación de servicio (DDoS) :

Es un tipo de ataque consiste en saturar con peticiones de servicio al servidor, hasta que éste no puede atenderlas, provocando su colapso.

Encriptar:

Proteger archivos expresando su contenido en un lenguaje cifrado. Los lenguajes cifrados simples consisten, por ejemplo, en la sustitución de letras por números.

IDS:

Un sistema de detección de intrusos (o IDS de sus siglas en inglés Intrusion Detection System) es una aplicación usada para detectar accesos no autorizados a un ordenador o a una red.

Incidente cibernético:

Es un intento organizado e intencionado causado por una o más personas para causar daño o problemas en un sistema informático o red, consiste en aprovechar una debilidad o falla en el software, en el hardware e incluso en las personas que forman parte de un ambiente informática, que compromete la confidencialidad, integridad o disponibilidad de la computadora o información almacenada en ella.

INEGI:

Es un organismo público autónomo responsable de normar y coordinar el Sistema Nacional de Información Estadística y Geográfica, así como de captar y difundir información de México en cuanto al territorio, los recursos, la población y economía, que permita dar conocer las características de nuestro país y ayudar a la toma de decisiones.

Ingeniería social:

Son tácticas utilizadas para obtener información datos de naturaleza sensible, en muchas ocasiones claves o códigos, de una persona. Estas técnicas de persuasión suelen valerse de la buena voluntad y falta de precaución de la víctima.

Internet:

Es una red de redes que permiten la interconexión descentralizada de computadoras a través de un conjunto de protocolos denominado TCP/IP.

IP:

Las direcciones IP (del acrónimo inglés IP para Internet Protocol) son un número único e irrepetible con el cual se identifica a todo sistema conectado a una red.

Glosario

IPS:

Intrusion Prevention System (sistema de prevención de intrusión) Es un software que se utiliza para proteger a los sistemas de ataques y abusos. La tecnología de prevención de intrusos puede ser considerada como una extensión de los sistemas de detección de intrusos (IDS), pero en realidad es una tecnología más cercana a los cortafuegos.

LAN:

Local Area Network: Red de Área Local. Red de computadoras interconectadas en un área reducida, por ejemplo, una empresa.

Malware:

Es un tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. Palabra que nace de la unión de los términos en inglés de software malintencionado: malicious software .

Página web:

Una de las páginas que componen un sitio de la WorldWideWeb. Un sitio web agrupa un conjunto de páginas afines. A la página de inicio se la llama "home page".

Phishing

Conocido como suplantación de identidad, es un término informático que denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta.

Política de seguridad:

Son las decisiones o medidas de seguridad que una empresa ha decidido tomar respecto a la seguridad de sus sistemas de información después de evaluar el valor de sus activos y los riesgos a los que están expuestos.

Producto Interno Bruto (PIB):

Es el valor monetario de los bienes y servicios finales producidos por una economía en un período determinado, es indicador representativo que ayuda a medir el crecimiento o decrecimiento de la producción de bienes y servicios de las empresas de cada país.

Ransomware:

Es un programa de software malicioso que infecta y restringe el acceso a un sistema y muestra mensajes exigiendo el pago de un rescate para reestablecer el funcionamiento del sistema, también es conocido como rogueware o sacreware. Los ataques más peligrosos han sido WannaCry, Petya, Cerber, Cryptolocker y Locky.

Red privada virtual:

Una red privada virtual, también conocida por sus siglas VPN (Virtual Private Network) es una conexión virtual punto a punto entre dos redes LAN usando para la conexión una red pública como es Internet y consiguiendo que esta conexión sea segura gracias al cifrado de la comunicación.

Spam:

Correo electrónico no solicitado. Se lo considera poco ético, ya que el receptor paga por estar conectado a Internet.

SSL:

Es un protocolo criptográfico seguro que proporciona comunicaciones seguras a través de una red (por ejemplo Internet). Generalmente comunicaciones cliente-servidor.

Virus informático:

Es un programa de código que se carga en un equipo de forma arbitraria, los cuales son diseñados para infectar y propagarse para tomar el control del sistema.

Vulnerabilidad informática

Es una debilidad o falla en un sistema de información que pone el riesgo la seguridad de la información, permitiendo que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad del a misma



**Secretaría de Seguridad y Protección Ciudadana
Guardia Nacional**

CERT-MX

Centro Nacional de Respuesta a Incidentes Cibernéticos

 **088**

 delitocibernetico_gn@sspc.gob.mx

 [@GN_MEXICO_](https://twitter.com/GN_MEXICO)

 [GUARDIA.NACIONAL.MX](https://www.facebook.com/GUARDIA.NACIONAL.MX)