GOBIERNO DEL PARAGUAY | MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GUÍA DE CIBERSEGURIDAD PARA PYMES

ENERO 2025

- **COVID-19:** Enfermedad infecciosa causada por el coronavirus SARS-CoV-2.
- **CERT-PY:** Equipo de Respuesta ante Incidentes Cibernéticos del Paraguay.
- **IA:** Inteligencia Artificial.
- **DDoS:** Denial of Service Distributed (Denegación de Servicio Distribuido). Este tipo de ataque consiste en inundar un servidor con una cantidad excesiva de tráfico, lo que hace que el servicio se vuelva inaccesible para los usuarios legítimos.
- **SQL:** Structured Query Language (Lenguaje de Consulta Estructurada). Es un lenguaje estándar para gestionar y manipular bases de datos relacionales.
- **IoT:** Internet of Things (Internet de las Cosas). Se refiere a la red de dispositivos físicos conectados a Internet y entre sí.
- **ISP:** Internet Service Provider (Proveedor de Servicios de Internet). Es una empresa que ofrece acceso a Internet a sus clientes.
- **WPA2:** Wi-Fi Protected Access 2. Es un protocolo de seguridad para redes inalámbricas, considerado más seguro que su predecesor, WPA. Se utiliza para asegurar las conexiones Wi-Fi.
- **WPS:** Wi-Fi Protected Setup. Es un protocolo de configuración que permite conectar dispositivos a una red Wi-Fi de forma rápida y sencilla, pero que también puede ser una vulnerabilidad si no se configura correctamente.
- **SSID:** Service Set Identifier. Es el nombre que se asigna a una red Wi-Fi y que es visible para los dispositivos que buscan conectarse.
- **SSL:** Secure Sockets Layer. Un protocolo de seguridad que proporciona autenticación y cifrado de comunicaciones de red. Aunque ha sido reemplazado en gran medida por TLS, todavía se puede encontrar en algunos sistemas.
- **HTTPS:** Hypertext Transfer Protocol Secure. Protocolo de comunicación seguro utilizado para la transmisión de datos en la World Wide Web. Es la versión segura del HTTP, y se utiliza para proteger las comunicaciones entre un servidor web y un navegador.
- **Wi-Fi:** Wireless Fidelity. Tecnología que permite la conexión inalámbrica a una red.
- **WPS:** Wi-Fi Protected Setup. Es un protocolo de configuración que permite conectar dispositivos a una red Wi-Fi de forma rápida y sencilla, pero que también puede ser una vulnerabilidad si no se configura correctamente.
- **AirDrop:** Es una función de dispositivos Apple (iPhone, iPad, iPod Touch y Mac) que permite compartir de forma inalámbrica archivos, fotos, vídeos, contactos y otros datos entre dispositivos cercanos.

ÍNDICE

Introducción

Muchas PYMEs, dependen significativamente de las TIC para sus operaciones, pero esta dependencia también las podría hacer vulnerables a ataques cibernéticos, si estos no son atendidos. La falta de medidas adecuadas de ciberseguridad podría provocar interrupciones graves, como el robo o bloqueo de datos sensibles y esenciales, daños a la reputación y otros.

Con la pandemia de COVID-19, muchas empresas adoptaron soluciones digitales apresuradas, lo que incrementó su exposición a riesgos. Esto no solo afecta a la empresa atacada, sino también a sus clientes, proveedores y socios, con consecuencias como la filtración de datos confidenciales o el robo de identidad.

Para enfrentar estos desafíos, el CERT-PY destaca la importancia de un enfoque integral en ciberseguridad, que no sólo proteja las operaciones internas, sino que también minimice los impactos en las redes externas. La guía busca equipar a las PYMES con estrategias prácticas para fortalecer su seguridad y garantizar la continuidad operativa.

La adopción de estas estrategias no solo fortalecerá la seguridad, sino que también contribuirá a la confianza y estabilidad a largo plazo en el entorno digital.

¿Qué es la ciberseguridad?

La ciberseguridad comprende un conjunto de procesos y estrategias destinados a proteger los sistemas y la información confidencial de las empresas contra los ciberataques y las filtraciones de datos. Los ciberataques son cada vez más complejos, y el panorama de las amenazas evoluciona: los ciberdelincuentes usan Inteligencia Artificial (IA) e ingeniería social para crear nuevos métodos de ataque. Como resultado, las empresas se ven forzadas a mejorar sus esfuerzos de ciberseguridad para adaptarse.

¿Por qué las PyMEs pueden ser vulnerables a los ciberataques?

- Gastan menos en ciberseguridad y pueden usar software desactualizado sin soporte técnico, convirtiéndose en objetivos fáciles.
- Permiten el uso de dispositivos personales, que son más susceptibles a malware y descargas maliciosas, aumentando el riesgo de ataques.

Entre las motivaciones de los ciberdelincuentes para dirigir sus ataques a PyMEs, se han identificado las siguientes:

1. **Dinero:** La principal motivación es la obtención de ganancias económicas. Es cierto que algunos ciberataques están inspirados en un deseo de venganza o de generar caos, pero la mayoría se lanzan para generar ganancias. Por ello, el ransomware es un método de ataque tan popular. En la medida en que un método de ataque sea lucrativo, los piratas informáticos seguirán usándolo.

2. **Potencia informática:** En ocasiones, los ciberdelincuentes reclutan los ordenadores de una empresa en un ejército de bots para lanzar ataques de

denegación de servicio distribuido (DDoS). Los ataques de DDoS implican la generación artificial de cantidades masivas de tráfico web para interrumpir el servicio que presta una empresa. Los bots secuestrados ayudan a generar tráfico molesto.

3. **Enlaces a otras entidades:** Las PyMEs están conectadas digitalmente con otras empresas a través de sus operaciones, las cadenas de suministro y la información que comparten. Como suele ser más difícil infiltrarse en las grandes empresas, los ciberdelincuentes apuntan a las pequeñas empresas como una forma de atacar los sistemas de las grandes

¿Qué tipos de ciberamenazas pueden afectar a las pequeñas empresas?

Antes de diagramar la estrategia de ciberseguridad de una PyMEs, se debe comprender cómo funciona el panorama de amenazas. Estas son algunas de las ciberamenazas que afectan a las pequeñas empresas:

1. Ingeniería social

Es un tipo de ciberdelito en el que se engaña o manipula a una persona para que divulgue información confidencial para fines fraudulentos. La ingeniería social puede adoptar distintas formas, por ejemplo:

1.1. Phishing

Un ciberdelincuente envía un correo electrónico engañoso para que el destinatario entregue información privada, o para implementar software malicioso en un dispositivo o en la red de la víctima.

1.2. Spear phishing

Una variante del phishing dirigido a una persona en particular, en la que el atacante se hace pasar por una persona conocida de la víctima.

1.3. Sitios web falsos

Diseñados para engañar a los usuarios con ataques maliciosos o fraudulentos.

1.4. Suplantación de identidad telefónica

Se produce cuando los estafadores cambian su identificador de llamadas para ocultar su identidad.

1.5. Smishing:

Una variante de phishing en la que se usan los teléfonos móviles para atacar la plataforma.

2. Ransomware

Es uno de los métodos más usados por los ciberdelincuentes para atacar empresas. Con el ransomware, se bloquean los ordenadores, se cifran los datos y se controla el sistema. Si los propietarios quieren recuperar el acceso a sus datos, deberán pagar un rescate a los ciberdelincuentes para que les envíen la clave de descifrado. Las PyMEs posiblemente recurrirán al pago del rescate si no cuentan con copias de seguridad de sus datos y necesitan volver a operar lo antes posible.

3. Malware

Es un término genérico con el que se refiere al software malicioso diseñado para hacer daño a los dispositivos o a la red de un usuario. Comprende una gran variedad de ciberamenazas, como troyanos y virus (de hecho, el ransomware es una forma de malware). Los ataques de malware son perjudiciales para las PyMEs porque pueden paralizar los dispositivos, lo que requiere reparaciones o reemplazos costosos. También pueden abrir una "puerta trasera" para que los atacantes accedan a los datos, lo que pone en riesgo tanto a los clientes como a los empleados.

4. Botnets

Un botnet es una red de ordenadores en peligro e infectados con malware, lo que permite a los atacantes combinar la potencia de procesamiento para ejecutar los ciberataques. Durante algún tiempo, fueron una amenaza para las grandes organizaciones, pero desde hace unos años, las pequeñas y medianas empresas también han sido víctimas.

5. Ataques de denegación de servicio distribuido

El objetivo de estos ataques es inundar un sitio web con tráfico de numerosas fuentes diferentes para que deje de funcionar. Un ataque de DDoS exitoso puede hacer que se desconecte por completo un sitio web, y que los clientes ya no puedan acceder a él.

6. Inserción de SQL

Si la empresa tiene una base de datos en SQL (lenguaje de consulta estructurado, en inglés), es potencialmente vulnerable a la inserción de SQL. Es un tipo de ataque en el que se inserta una parte de un código malicioso en una base de datos SQL. Dependiendo de la naturaleza del código malicioso, las consecuencias pueden ser muy graves. Por ejemplo, puede eliminar los datos, comprometer la información confidencial del usuario y, en casos extremos, apagar todo el sistema. Es una de las formas más habituales de ataque a un sitio web.

¿Por qué es esencial la ciberseguridad para las PyMEs?

Son diversos los motivos por los que se debe tomar en serio la ciberseguridad para pequeñas empresas y la seguridad para PyMEs, entre ellos:

1. **La posibilidad de pérdidas financieras:**

   Un incidente cibernético puede destruir las finanzas de las pequeñas empresas, en ocasiones, de forma definitiva. El coste de la recuperación, la pérdida de ingresos durante el período de inactividad y las sanciones financieras por el incumplimiento de la legislación pueden afectar los resultados de la empresa.

2. **Daño a la reputación:**

   En función de la escala del ataque y de cómo se maneje, si el negocio sufre una filtración de datos que afecta la información del cliente, el impacto en la reputación de la empresa puede ser muy grave. Esto puede afectar tu capacidad para retener y atraer a nuevos clientes y empleados.

3. **Poner a los empleados en riesgo:**

   Si los ciberdelincuentes roban información confidencial de los empleados, como archivos de RR. HH. confidenciales, fechas de nacimiento, información financiera, etc., estos estarán expuestos al riesgo de robo de identidad y otros ciberdelitos.

4. **Capacidad para seguir operando:**

   Las empresas de todos los tamaños confían plenamente en los sistemas informáticos, en especial, desde la pandemia de la COVID-19. La confianza en los servicios en la nube, en teléfonos inteligentes, en el Internet de las cosas y en la inteligencia artificial significa que cualquier interrupción provocada por un ciberataque impide que una empresa opere con normalidad.

¿Cómo puedes proteger a las PyMEs de las ciberamenazas?

Para proteger las PyMEs de ciberamenazas, es clave desarrollar una estrategia de ciberseguridad. Esto incluye capacitar a los empleados para que verifiquen antes de confiar y limitar su acceso solo a la información necesaria para sus funciones.

Se recomienda crear perfiles de usuario con permisos específicos y, cuando no sea posible, restringir y proteger con contraseñas el acceso a archivos y carpetas dentro del sistema.

Aspectos clave a considerar:

1. **Cuentas de usuarios.**

Después de comprender cuál es la información de la empresa y cómo puede poner en riesgo a la organización, las empresas deben identificar quién tiene acceso a qué datos.

Las empresas deben gestionar el acceso a sus sistemas con un enfoque estructurado:

- **Inventario de cuentas:** Identificar y registrar todas las cuentas de usuario en servicios, dispositivos y plataformas, incluyendo proveedores externos con acceso.

- **Control de acceso:** Asignar permisos según funciones y exigir contraseñas únicas para cada sistema, priorizando aquellos con información sensible.
- **Seguridad de cuentas:** Prohibir el uso compartido de credenciales y proteger los datos críticos con contraseñas seguras y cifrado.

2. Instalar un software antivirus y antimalware confiable

Instalar un software antivirus y antimalware confiable es esencial para protegerse contra amenazas. Aunque los sistemas operativos incluyen protección básica, los ciberdelincuentes desarrollan malware que evade estas defensas. Por ello, es recomendable contar con una solución de seguridad adicional y mantenerla siempre actualizada.

3. Usar cortafuegos de red

Utilizar cortafuegos es clave para controlar el tráfico de red y proteger la empresa de accesos no autorizados. Pueden estar integrados en el enrutador del proveedor de Internet o en programas antivirus. Según el nivel de riesgo, es recomendable actualizarlos y complementarlos con cifrado y monitoreo del tráfico.

4. Utilizar contraseñas seguras

Crear contraseñas robustas y únicas. Una contraseña robusta debe tener al menos 16 caracteres combinando letras mayúsculas, minúsculas, números y caracteres especiales. **Ejemplos de ese tipo de contraseñas:** #Sl33pWe11000$&*

4.1. Protección de contraseñas

Las contraseñas siempre deben ser:

1. **Complejas:** Utilizar una combinación de al menos 16 caracteres, combinando letras mayúsculas, minúsculas, caracteres especiales.

2. **Guardadas en un lugar seguro:** Se recomienda el uso de gestores de contraseñas, herramientas diseñadas para almacenar y cifrar contraseñas de forma segura. Evite escribirlas en documentos físicos o digitales desprotegidos.

3. **Confidenciales:** No compartirlas ni anotarlas en lugares visibles o accesibles, como notas adhesivas o documentos cercanos al área de trabajo.

4. **Cambiadas regularmente:** Actualizarlas cada 90 días, o al menos una vez al año, según las necesidades de seguridad.

5. **Contraseñas únicas:** Cada sistema o sitio debe tener su propia contraseña.

Una de las vulnerabilidades más comunes en las empresas es que los empleados escriben sus contraseñas en notas visibles o documentos no protegidos. Esto compromete la seguridad de los datos y puede ser fácilmente explotado.

Para mitigar este riesgo:

- **Usar gestores de contraseñas:** Estas herramientas permiten a los usuarios generar y almacenar contraseñas únicas para cada sistema o sitio web. Además, protegen la información mediante cifrado avanzado.

- **Evitar guardar contraseñas en navegadores:** Aunque es una opción conveniente, guardar contraseñas en navegadores representa un riesgo porque pueden ser vulnerables a ataques y accesos no autorizados. Los gestores de contraseñas ofrecen una alternativa más confiable y segura.

Las interfaces administrativas de los sistemas suelen incluir opciones para personalizar los requisitos de contraseña. Las empresas deben utilizar estas funciones para:

- Establecer longitudes mínimas y criterios de complejidad.
- Configurar frecuencias obligatorias para el cambio de contraseñas.
- Crear especificaciones alineadas con los estándares de seguridad deseados.

5. Utilizar la Autenticación multifactor

La autenticación multifactor requiere que los usuarios proporcionen dos o más formas de verificación para acceder a una cuenta o sistema, como una contraseña y un código enviado por el sistema (correo electrónico, mensaje de texto, llamada telefónica). Es común en plataformas tecnológicas, como sistemas de pago y cuentas de usuario. Las empresas deben asegurarse de habilitarla tanto para cuentas internas (empleados) como externas (clientes), cuando sea posible, ya que la activación del mismo añade una capa de seguridad a sus sistemas.

6. Actualizar el software de manera regular

Las actualizaciones de software solucionan vulnerabilidades de seguridad conocidas en aplicaciones, programas o sistemas operativos, por lo que deben instalarse lo antes posible. Aunque las actualizaciones corrigen problemas detectados, si una vulnerabilidad no es identificada, la empresa seguirá siendo vulnerable. Sin embargo, mantener el software actualizado regularmente ayuda a mitigar gran parte de este riesgo.

7. Cifrar todos los datos confidenciales

El cifrado de datos asegura que solo quienes tienen las claves o contraseñas puedan acceder a la información. Se puede cifrar archivos o dispositivos completos, incluidas las unidades en la nube. Herramientas como BitLocker (Microsoft) y FileVault (Apple) permiten cifrar datos, pero si se pierde la clave o contraseña, los datos no se pueden recuperar. Es importante guardar la clave en un lugar seguro o recordar la contraseña de manera segura.

8. Asegurar las conexiones Wi-Fi

Para asegurar las conexiones Wi-Fi en empresas:

- Cambiar la contraseña de acceso al enrutador y guardarla de forma segura.
- Actualizar regularmente el firmware del enrutador.
- Habilitar el protocolo de encriptación Wi-Fi más avanzado (como WPA2) y cambiar las contraseñas con frecuencia.
- Deshabilitar la conexión Wi-Fi fácil (como WPS) para evitar accesos no autorizados.
- Cambiar el nombre del Wi-Fi (SSID) para no revelar información sobre el dispositivo o ISP.
- Probar los cambios para asegurar que funcionan correctamente.
- Agregar tu propio enrutador para mejorar la seguridad y control sobre la red.

9. Mantener el sitio web de la empresa seguro

Para mantener seguro el sitio web de una empresa, es importante considerar sus propiedades técnicas, el ecosistema de TI en el que se administra y su lugar de alojamiento. Aunque muchos utilizan servicios en la nube que facilitan la creación y administración del sitio, delegando parte de la seguridad al proveedor, los sitios web siguen siendo vulnerables si el código, los complementos, las extensiones o servicios de terceros están mal configurados o tienen fallas de seguridad.

9.1. Para asegurar un sitio web empresarial, considerar los siguientes aspectos:

- **Credenciales seguras:** Establecer requisitos estrictos para las contraseñas de administradores y limite el número de usuarios con privilegios de administrador.
- **Software confiable:** Utilizar plataformas de creación y alojamiento de buena reputación con funciones de seguridad integradas (como cortafuegos, antimalware y protección contra ataques DDoS).
- **Actualizaciones regulares:** Mantener al día la plataforma, los complementos y las integraciones de terceros.
- **Protocolos HTTPS:** Instalar certificados SSL para cifrar la información entre el sitio y los usuarios.
- **Seguridad de cuentas de usuario:** Solicitar contraseñas seguras y habilite el bloqueo de cuentas tras múltiples intentos fallidos.
- **Protección de archivos cargados:** Implementar escáneres antivirus, limite el tipo y tamaño de archivos y almacénelos en ubicaciones seguras.

- **Copias de seguridad periódicas:** Realizar copias diarias y considere copias de seguridad redundantes en diferentes ubicaciones para mayor protección ante desastres o ataques cibernéticos.

10. Evitar que los teléfonos móviles sean objetivos de ataque

Los teléfonos móviles almacenan datos personales y laborales y están siempre en línea, lo que los hace vulnerables a pérdidas, robos o ataques de malware, poniendo en riesgo la red de una empresa. Las empresas tienen más control sobre los dispositivos que proporcionan a sus empleados que sobre los dispositivos personales que estos utilizan en el entorno laboral.

10.1. Para asegurar dispositivos móviles en entornos empresariales:

- Utilizar el sistema operativo del fabricante y manténgalo actualizado. Evite rooting o jailbreaking para mantener la seguridad.
- Cifrar la información almacenada y use contraseñas seguras o biometría para desbloquear el dispositivo.
- Evitar enlaces sospechosos en aplicaciones de mensajería o texto para prevenir malware.
- Controlar las aplicaciones: Instale solo desde tiendas oficiales y limite sus permisos (ubicación, contactos, cámara, etc.).
- Desactivar funciones innecesarias (Bluetooth, Wi-Fi, AirDrop) para reducir posibles vías de ataque.
- Eliminar datos empresariales al desconectar un dispositivo de la red corporativa, idealmente limpiando por completo el teléfono.

11. Mantener copias de seguridad de toda la información

Para mantener copias de seguridad seguras, PYMEs deben:

- Priorizar la información confidencial y los sistemas críticos al hacer copias de seguridad.
- No depender solo del almacenamiento en la nube, ya que sincronizar datos puede propagar ataques. Utilizar soluciones en la nube de buena reputación como paso inicial, pero entender sus limitaciones (por ejemplo, tamaño de archivos, nombres incompatibles y posibles pérdidas entre copias).
- Crear imágenes completas de discos duros, incluyendo programas y sistemas operativos, para una recuperación rápida tras un incidente.
- Usar estrategias híbridas: combinar almacenamiento local y en la nube para mayor seguridad.

11.1. Respaldo de datos

Las PYMEs deben tener en cuenta ciertos aspectos claves:

- Realizar copias de seguridad frecuentes, preferiblemente automáticas. Si no es posible, asignar tiempo para copias manuales completas.
- Usar múltiples copias en diferentes medios para evitar corrupción o pérdida, y guardar una copia fuera del sitio para protegerla de desastres.
- Cifrar todas las copias para mayor seguridad.
- Considerar la falta de estandarización en sistemas y dispositivos; si no pueden unificarlos, hacer copias manuales o invertir en infraestructura de TI compatible.

Conclusión

Esta guía de ciberseguridad para PyMEs destaca la importancia de protegerse contra ciberamenazas crecientes, enfatizando la vulnerabilidad de las PyMEs debido a recursos limitados y el uso de tecnología desactualizada. Ofrece un enfoque integral para fortalecer la seguridad mediante estrategias como capacitación de empleados, gestión de accesos, uso de software antivirus, contraseñas seguras, autenticación multifactor y cifrado de datos. Además, resalta la importancia de mantener actualizados los sistemas, proteger redes Wi-Fi, asegurar sitios web y dispositivos móviles, y realizar copias de seguridad frecuentes para garantizar la continuidad operativa.

Fuente

- https://www.marketlinks.org/sites/default/files/media/file/2022-09/072822_Cyber%20Guidebook_Spanish_P1_B.pdf
- https://pdf.usaid.gov/pdf_docs/PA00ZKCQ.pdf