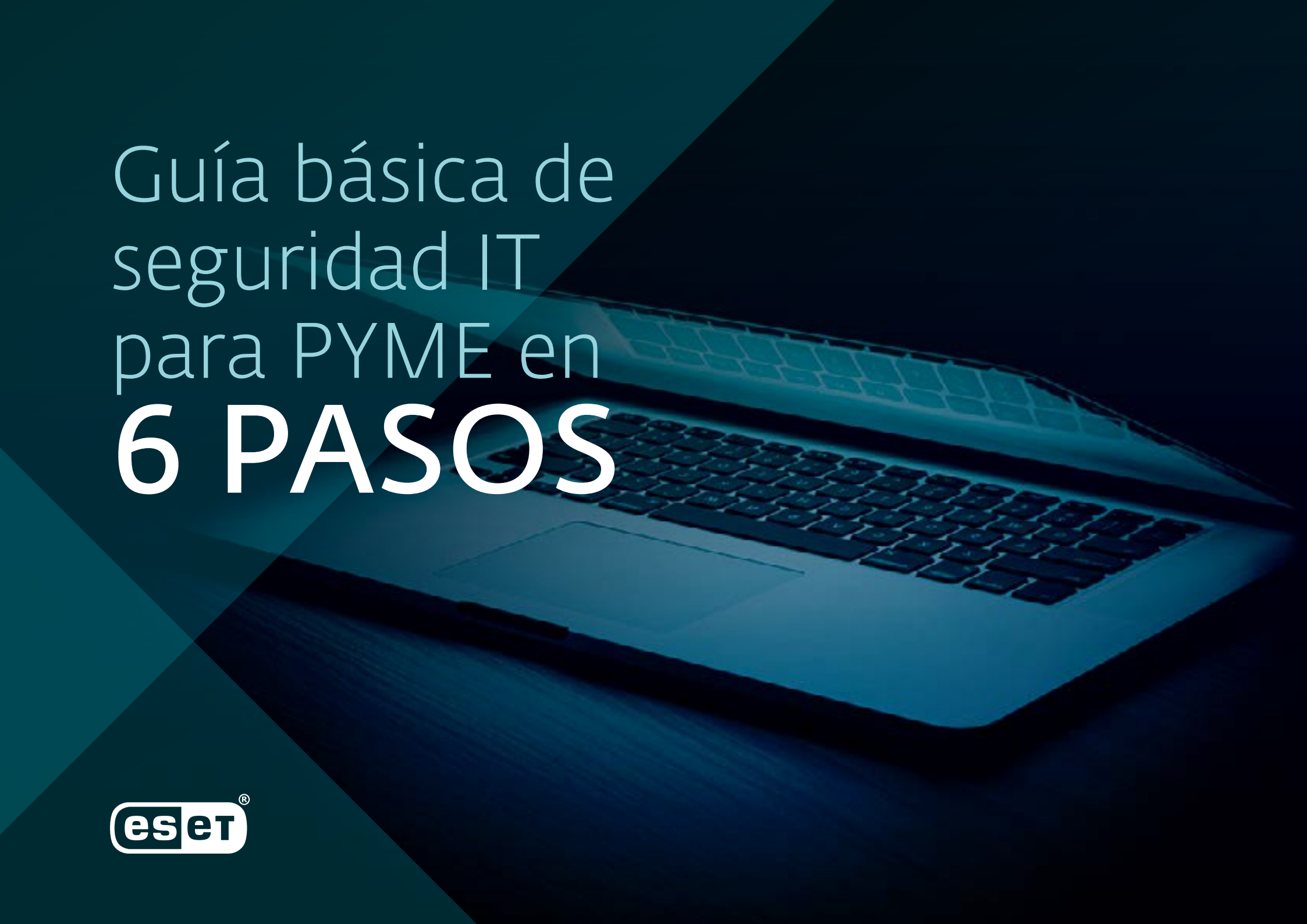
Guía básica de seguridad IT para PYME en 6 PASOS



GUÍA BÁSICA DE SEGURIDAD IT PARA PYME EN 6 PASOS

Si bien las computadoras e Internet ofrecen muchos beneficios a las pequeñas empresas, estas tecnologías no están exentas de riesgos. Algunos de ellos, como el robo físico de equipos y los desastres naturales, se pueden reducir o controlar con conductas sensatas y precauciones de sentido común. Pero los riesgos resultantes del crimen cibernético, como el robo de información personal que luego se vende en el mercado negro, son más difíciles de manejar.

A pesar de que el 63% de las pequeñas y medianas empresas experimentaron una vulneración de datos durante 2019, muchos propietarios aún creen que son inmunes a los ciberataques debido a su pequeño tamaño y activos limitados. Pero lamentablemente están equivocados.

Esta guía lo ayudará a defender su empresa ante las amenazas del crimen cibernético.

La información personal es uno de los objetivos más comunes de los delincuentes. Incluso las empresas más pequeñas manejan datos personales de clientes o proveedores que les pueden interesar robar. Otro objetivo popular de los ciberdelincuentes es la información de cuentas, que incluye datos de tarjetas de crédito, números de cuentas bancarias, contraseñas de banca online, cuentas de correo electrónico y credenciales de usuario para servicios como eBay, PayPal y TurboTax.

Una vez que obtienen los datos, los venden en el mercado negro a otros delincuentes que se dedican a usar dicha información para llevar a cabo una amplia variedad de fraudes y estafas.

de los ataques cibernéticos se dirigieron a pequeñas empresas

de las pequeñas y medianas empresas experimentaron ocho horas o más de inactividad debido a una vulneración cibernética

Fuente: Agility SMB

CONSECUENCIAS DEL ROBO DE DATOS

Como casi todas las pequeñas empresas, la suya seguramente también manejará información de cuentas y datos personales de interés para los delincuentes. Por eso, debe recordar que su empresa será considerada responsable de las consecuencias del robo de datos, por ejemplo, si los criminales extraen información de sus clientes y la utilizan para cometer fraudes.

Algunos datos están protegidos por leyes y reglamentos, como el reglamento GDPR en la Unión Europea o la ley CCPA en California, Estados Unidos. Muchos estados también obligan a las empresas a informar si sufren una vulneración de seguridad que exponga datos personales a posibles abusos, ya sea por la pérdida de una computadora portátil con información de clientes o de una memoria USB con registros médicos.

Esto implica que, por más que su empresa sea pequeña, debe adoptar un enfoque sistemático para proteger los datos que se le confían. Además, a medida que vaya protegiendo los activos digitales corporativos, deberá documentar el enfoque implementado. Esto lo ayudará a capacitar a los empleados sobre sus responsabilidades en materia de seguridad.

También es muy común que las empresas más grandes les exijan a los proveedores y contratistas pruebas de que han capacitado a sus empleados e implementado las medidas de seguridad pertinentes. De esta forma, si se llegara a producir una vulneración de seguridad, esta documentación de las políticas aplicadas lo ayudará a demostrar que fue diligente en sus esfuerzos para proteger la información.

Un tercio de los gastos generados por una vulneración de datos se producen más de un año después del incidente. Alrededor del 22% de estos gastos se producen durante el segundo año.

Fuente: ENISA

PASOS A SEGUIR:

Los siguientes seis pasos lo ayudarán a proteger su empresa ante las amenazas de seguridad cibernética.

A) **Analizar activos, riesgos y recursos;**

B) **Crear políticas;**

C) **Elegir controles;**

D) **Implementar controles;**

E) **Capacitar empleados, directivos y vendedores;**

F) **Seguir evaluando, auditando y probando.**

ANALIZAR ACTIVOS, RIESGOS Y RECURSOS

ANALIZAR ACTIVOS, RIESGOS Y RECURSOS

Realiza una lista con todos los sistemas y servicios informáticos que utiliza. Asegúrese de incluir los dispositivos móviles que tanto usted como sus empleados pueden llegar a usar para acceder a información corporativa o de los clientes.

Esto es especialmente importante, ya que el **62% de 1.100 profesionales** encuestados declararon que decidieron prescindir de la seguridad móvil en aras de la eficiencia[1].

Incluya los servicios online, como SalesForce, los sitios web de banca online y los servicios en la nube, como iCloud o Google Docs.

Luego, lea la lista y piense en los riesgos relacionados con cada elemento. *¿Quién o qué es la amenaza? ¿Cuáles son los riesgos asociados al trabajo a distancia? Otra buena pregunta es:* **¿Qué podría salir mal?** Algunos riesgos son más probables que otros: clasifíquelos y enumérelos según el daño que podrían causar y su probabilidad de ocurrencia.

Es posible que necesite buscar ayuda externa para este proceso, por lo cual deberá hacer otra lista con los **recursos que tenga disponibles para resolver los problemas de seguridad IT.** Estos recursos podrían ser algún empleado, partner o vendedor con conocimientos sobre seguridad. También puede contratar a un proveedor de servicios gestionados (MSP) externo para que se encargue de una parte o la totalidad de su seguridad cibernética y le proporcione el apoyo que necesite en todo momento.

62%

de los profesionales admitieron que prefirieron prescindir de la seguridad móvil en aras de la eficiencia

1) Fuente: Cyber Talk, marzo de 2020

3

CREAR POLÍTICAS

CREAR POLÍTICAS

Un programa de seguridad sólido comienza con la aplicación de políticas, y para ello se necesita que **los directivos de la empresa las aprueben**. Si usted es el jefe, debe informarles a todos que se toma en serio la seguridad y que su empresa se compromete a proteger la privacidad y la seguridad de todos los datos que maneja.

A continuación, debe detallar las políticas que desea aplicar, por ejemplo, que **no se permite el acceso no autorizado a los sistemas y datos corporativos**, y que los empleados no deben desactivar la configuración de seguridad en sus dispositivos móviles.

Debe definir quién tiene acceso a qué datos dentro de la organización, con qué fin y qué están autorizados a hacer con ellos. También es importante contar con políticas para el acceso remoto, el uso de dispositivos propios para trabajar (BYOD) y el software autorizado.

ELEGIR CONTROLES

ELEGIR CONTROLES

Use controles para hacer cumplir las políticas. Por ejemplo, **si desea aplicar una política para impedir el acceso no autorizado** a los sistemas y datos corporativos, puede optar por controlar todo el acceso a los sistemas de la empresa mediante la solicitud de un nombre de usuario y contraseña, y un **segundo factor de autenticación (2FA).**

Para controlar **qué programas tienen permiso** de ejecutarse en los equipos de la empresa, puede decidir no darles a los empleados **derechos de administrador**. Para evitar las filtraciones causadas por dispositivos móviles perdidos o robados, podría exigirles a los empleados que informen sobre estos incidentes en el mismo día, y bloquear el dispositivo afectado para borrar su contenido de inmediato en forma remota.

Debería utilizar las siguientes tecnologías de seguridad:

- **Protección para endpoints** para evitar que se descarguen códigos maliciosos en sus dispositivos;
- **Cifrado** para proteger los datos de los dispositivos robados (también sugerido en el reglamento GDPR);
- **2FA** para requerir algo más que un nombre de usuario y una contraseña al acceder a sus sistemas y datos;
- **Solución VPN** para una protección adicional.

Prepare la seguridad informática de su empresa para el futuro

El panorama actual de ciberseguridad está en continua evolución y las amenazas utilizan técnicas de ofuscación cada vez más sofisticadas. El objetivo final de los actores del malware es pasar desapercibidos en las endpoints, evadiendo la detección antimalware mediante la creación de amenazas nunca antes vistas, o 0-day.

Un producto de seguridad con sandboxing basado en la nube proporciona una capa de defensa fuera de la red corporativa para evitar que el ransomware se llegue a ejecutar en el entorno de producción. Impide que el archivo sospechoso se ejecute en la endpoint.

IMPLEMENTAR CONTROLES

IMPLEMENTAR CONTROLES

Cuando implemente los controles, asegúrese de que funcionan correctamente. Por ejemplo, debería tener una política que prohíba el uso de software no autorizado en los sistemas de la empresa. Entonces, uno de los los controles será el **software antimalware** que busca códigos maliciosos.

No solo debe instalarlo y probar que no interfiera con las operaciones comerciales normales, sino que también tiene que documentar los procedimientos que los empleados deberán seguir en caso de que el software detecte malware.

Cuando elija la solución de protección para endpoints adecuada, también hay que tener en cuenta algunas consideraciones clave. Por ejemplo, es importante que tenga los **mayores índices de detección posibles**, mientras que la incidencia de falsos positivos (alertas sobre los archivos o enlaces que no son realmente maliciosos) debe ser lo más cercana a cero. **Tampoco debería tener un impacto notable en el rendimiento del sistema, y debería ser fácil de gestionar y mantener**.

Consola de administración de seguridad para endpoints

Al implementar la protección de endpoints, es importante tener una visión general de todas las endpoints en una misma pantalla. Una consola en la nube como ESET PROTECT ofrece esta funcionalidad.

Garantiza la visibilidad en tiempo real de las endpoints locales y externas, y permite gestionar la seguridad y generar informes completos para todos los sistemas operativos.

Controla las funciones de prevención, detección y respuesta en las endpoints de todas las plataformas (incluyendo los equipos de escritorio, los servidores, las máquinas virtuales e incluso los dispositivos móviles gestionados).

MÁS INFORMACIÓN

CAPACITAR EMPLEADOS, DIRECTIVOS Y VENDEDORES

CAPACITAR EMPLEADOS, DIRECTIVOS Y VENDEDORES

Sus empleados necesitan saber algo más que las políticas y procedimientos de seguridad de la empresa. También deben entender por qué son necesarios. Esto implica **invertir en capacitación y concientización sobre seguridad**: la medida más importante y efectiva que una empresa puede implementar.

Por ejemplo, al trabajar con sus empleados, genere conciencia sobre temas como los correos electrónicos de phishing. Un estudio mostró que el 43% de los empleados ni siquiera están seguros de qué es un ataque de phishing[2].

Por lo tanto, prepare capacitaciones periódicas, por ejemplo, un cuestionario sobre phishing, para enseñarles qué técnicas están utilizando los actores maliciosos. Haga que la concientización sobre seguridad cibernética sea parte del proceso de incorporación de nuevos empleados y proporcione consejos de seguridad en una página de intranet.

Asegúrese de capacitar a todos los que usen sus sistemas, incluyendo directivos, vendedores y partners. Y **recuerde que el incumplimiento de las políticas de seguridad debe tener consecuencias estrictas**, ya que socava todo el esfuerzo de seguridad.

69%

de las organizaciones sufrieron una vulneración debido a una amenaza interna, a pesar de las medidas preventivas[3]

2) Fuente: ZD Net, octubre de 2020
3) Fuente: Sapio Research Study, Reino Unido

SEGUIR EVALUANDO, AUDITANDO Y PROBANDO

SEGUIR EVALUANDO, AUDITANDO Y PROBANDO

Para cualquier empresa la seguridad IT es un proceso continuo, no un proyecto que se ejecuta una sola vez.

Es posible que necesite **actualizar sus políticas de seguridad y sus controles más de una vez al año**, dependiendo de los cambios en la empresa, como las relaciones con nuevos vendedores, nuevos proyectos, incorporaciones de empleados o empleados que dejan la empresa (siempre asegurándose de que se revoquen todos sus accesos al sistema cuando se van). Considere contratar a un consultor externo para realizar una prueba de penetración y una auditoría de seguridad para detectar los puntos débiles y poder abordarlos.

Por lo que podemos ver, la ola de delitos informáticos no va a parar en el futuro cercano, de modo que debe hacer un esfuerzo continuo de buena fe para proteger los datos y los sistemas, que son el alma de las pequeñas empresas de hoy.

Infórmese sobre las amenazas emergentes, en sitios web como:

WeLiveSecurity.com/latam

DataSecurityGuide.eset.com

Por más de 30 años, ESET® ha estado desarrollando soluciones de seguridad líderes en la industria para las empresas y los consumidores de todo el mundo. Con las soluciones de seguridad que van desde la protección de endpoints y dispositivos móviles, hasta el cifrado y la autenticación en dos fases, los productos de alto rendimiento y fáciles de usar de ESET les ofrecen a los usuarios y a las empresas la tranquilidad que necesitan para disfrutar de su tecnología a pleno. ESET brinda protección y supervisión en forma discreta las 24 horas, los 7 días de la semana, y actualiza las defensas en tiempo real para mantener a los usuarios seguros y a las empresas funcionando sin interrupciones. Para obtener más información, visite www.eset.com/latam.