

# 6-PASOS

Guía de iniciación  
a la ciberseguridad  
para PYMES



## CIBERSEGURIDAD EN 6 PASOS. GUÍA DE INICIO PARA LAS PYMES

Los ordenadores e Internet aportan muchas ventajas a las pequeñas empresas, pero esta tecnología no está exenta de riesgos. Algunos riesgos, como los robos físicos y las catástrofes naturales, pueden reducirse o controlarse mediante un comportamiento sensato y precauciones de sentido común.

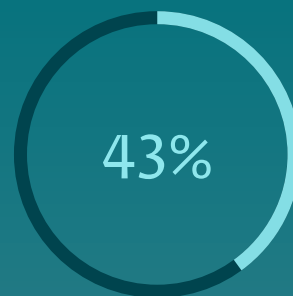
Más difíciles de manejar son los riesgos de la ciberdelincuencia, como los que roban información para venderla en el mercado negro.

**El 63% de las pequeñas/medianas empresas experimentaron una vulneración de datos en 2019**, según un informe del Instituto Ponemon. Sin embargo, muchos propietarios creen que no son vulnerables a los ciberataques debido a su pequeño tamaño y sus limitados activos. Por desgracia, esto no es así.

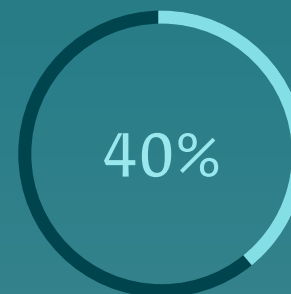
Esta guía te ayudará a defender tu negocio contra las amenazas de la ciberdelincuencia.

**La información personal es un objetivo habitual** de los delincuentes. Incluso las empresas más pequeñas suelen manejar algunos datos personales de clientes o proveedores que merecen ser robados. Otro objetivo popular de los ciberdelincuentes es la información de las cuentas, incluidos los datos de las tarjetas de crédito, los números de las cuentas bancarias, las contraseñas de la banca online, las cuentas de correo electrónico y las credenciales de usuario de servicios como eBay, PayPal y TurboTax.

Todo ello puede venderse en el mercado negro a otros delincuentes especializados en utilizar la información en una amplia gama de esquemas de fraude y estafas.



de los ciberataques se dirigen a las pequeñas empresas



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

## CONSECUENCIAS DEL ROBO DE DATOS

Dado que la mayoría de las pequeñas empresas tienen información de cuentas y datos personales de los que los delincuentes podrían abusar, debes recordar que tu empresa puede ser responsable de las consecuencias del robo de datos, por ejemplo, si la información sobre tus clientes es robada y utilizada para el fraude.

Algunos datos están protegidos por leyes y reglamentos, como el **GDPR en la UE o la CCPA en California, U.S.A.** Muchos estados también exigen a las empresas que informen de las fugas de seguridad que exponen los datos personales a posibles abusos, ya sea un ordenador portátil perdido con datos de clientes o una memoria USB con historiales médicos.

Todo esto significa que, aunque tu empresa sea pequeña, debes adoptar un **planteamiento sistemático para proteger los datos** que se te confían. A medida que vayas protegiendo los activos digitales de tu empresa, deberás documentar tu planteamiento. Esto te ayudará a **formar a los empleados** sobre sus responsabilidades en materia de seguridad.

Además, no es raro que las grandes empresas exijan a los proveedores y empresas contratistas que demuestren que han formado a sus empleados en materia de seguridad y que han puesto en marcha las medidas de seguridad adecuadas. Si se produce una vulneración de la seguridad, una política de seguridad documentada te ayudará a demostrar que has sido riguroso en tus esfuerzos por proteger la información.

**Un tercio** de los costes relacionados con una vulneración de datos se producen más de un año después del incidente. Alrededor del **22%** de estos costes se producen en el segundo año.

## PASOS A SEGUIR:

Hemos elaborado un planteamiento sistemático de la ciberseguridad:

- Evalúa tus activos, riesgos y recursos
- Construye tu política
- Elige tus controles
- Implementa controles
- Forma a tus empleados, ejecutivos y proveedores
- Sigue evaluando, auditando y probando



RANSOMWARE

EVALÚA TUS  
ACTIVOS, RIESGOS  
Y RECURSOS

# EVALÚA TUS ACTIVOS, RIESGOS Y RECURSOS

**Enumera todos los sistemas y servicios** informáticos que utilizas. Al fin y al cabo, si no sabes lo que tienes, no puedes protegerlo. Asegúrate de incluir los dispositivos móviles, como teléfonos inteligentes y tabletas, que tú y/o tus empleados puedan utilizar para acceder a la información de la empresa o de los clientes.

Esto es especialmente **importante: el 62% de los 1.100 profesionales encuestados** declararon que dejaban de lado la seguridad móvil en beneficio de la eficiencia.<sup>1</sup>

Y no hay que olvidar los servicios online, como Salesforce, los sitios web de banca online y los servicios en la nube como iCloud o Google Docs.

Ahora revisa esa lista y considera los riesgos relacionados con cada elemento. ¿Quién o qué es la amenaza? ¿Cuáles son los riesgos relacionados con el trabajo a distancia? Otra buena pregunta es **¿qué podría salir mal?** Algunos riesgos son más probables que otros, pero haz una lista de todos ellos y luego clasifícalos según el daño que podrían causar y las posibilidades de que se produzcan.

Es posible que busques ayuda externa para este proceso, por lo que necesitas otra lista: **los recursos a los que puedes recurrir para cuestiones de ciberseguridad.** Puede tratarse de alguien de la plantilla con conocimientos y experiencia en seguridad, o de un proveedor o distribuidor. También puedes subcontratar tu ciberseguridad a un proveedor de servicios gestionados (MSP) que pueda proporcionarte el apoyo que necesitas.

El **62%**  
de los profesionales  
admite que deja de  
lado la seguridad  
móvil en beneficio  
de la eficiencia

A group of business professionals are gathered around a table in a modern office, working on laptops. The scene is dimly lit, with the primary light source being the screens of the laptops and the ambient light from a large window overlooking a city skyline at night. The office environment is contemporary, with sleek furniture and a professional atmosphere. The overall color palette is dominated by dark blues and greys, with the city lights providing a warm, bokeh effect in the background.

CONSTRUYE  
TU POLÍTICA

# CONSTRUYE TU POLÍTICA

Un programa de seguridad sólido comienza con una política, y la política comienza con la **aceptación del nivel C**. Si eres el jefe, tienes que hacer saber a todos que te tomas la seguridad en serio y que tu empresa se compromete a proteger la privacidad y la seguridad de todos los datos que maneja.

A continuación, tienes que detallar las políticas que quieres aplicar, por ejemplo, no habrá **acceso no autorizado a los sistemas y datos de la empresa**, y los empleados no podrán desactivar la configuración de seguridad de sus dispositivos móviles.

Hay que definir quién tiene acceso a determinados datos dentro de una empresa, con qué fines y qué está autorizado a hacer con esos datos. También es importante contar con políticas sobre el acceso remoto, el programa "trae tu propio dispositivo" (BYOD) o el software autorizado.







ELIGE TUS  
CONTROLES

# ELIGE TUS CONTROLES

Los controles se utilizan para aplicar las políticas. Por ejemplo, para **hacer cumplir la política de no acceder sin autorización** a los sistemas y datos de la empresa, puedes optar por controlar todos los accesos a los sistemas de la empresa con un nombre de usuario único, una contraseña y alguna forma de autenticación de dos factores.

Para controlar **qué programas se pueden ejecutar** en los ordenadores de la empresa, puedes decidir no dar a los empleados **derechos administrativos**. Para evitar las infracciones causadas por la pérdida o el robo de dispositivos móviles, puedes exigir a los empleados que informen de estos incidentes el mismo día, y especificar que dichos dispositivos se bloquearán y borrarán de forma remota inmediatamente.

Como mínimo, deberás utilizar estas tecnologías de seguridad:

- **Solución de protección de equipos** que evitará que se descargue código malicioso en tus dispositivos.
- **Un software de cifrado** que haga inaccesibles los datos de los dispositivos robados, algo que también sugiere el GDPR de la UE.
- **Un sistema de autenticación de dos factores**, de modo que se requiera algo más que un nombre de usuario y una contraseña para acceder a tus sistemas y datos.
- **Una solución VPN** que añada otra capa de protección a los empleados que trabajan a distancia.

## La seguridad informática de tu empresa a prueba de fallos

El entorno actual de la ciberseguridad está en continua evolución, utilizando sofisticadas técnicas de ofuscación. El objetivo final de los atacantes de malware es pasar desapercibidos en el equipo, evadiendo la detección antimalware mediante la creación de amenazas nunca antes vistas, o de día cero.

Una sandbox de seguridad basada en la nube proporciona una capa defensiva fuera de la red de la empresa para evitar que el ransomware se ejecute en un entorno de producción. Se bloquea la ejecución del archivo sospechoso en el equipo.



# IMPLEMENTA

Cuando implementes los controles, asegúrate de que funcionan. Por ejemplo, debes tener una política que prohíba el software no autorizado en los sistemas de la empresa; uno de tus controles será **un software antimalware** que busque código malicioso.

No solo tienes que instalarlo y probar que no interfiere en las operaciones normales de la empresa, sino que también tienes que documentar los procedimientos que quieres que sigan los empleados cuando se detecte código malicioso.

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

## Consola de gestión de la seguridad de los equipos

Cuando se implementa la protección de los equipos, se desea tener una visión general de todos tus equipos en un único panel de control. Una consola en la nube como ESET PROTECT ofrece esta funcionalidad.

Garantiza la visibilidad en tiempo real de los equipos locales y externos, así como la elaboración de informes completos y la gestión de la seguridad para todos los sistemas operativos.

Controla la prevención, la detección y la respuesta de los equipos en todas las plataformas, incluyendo ordenadores de sobremesa, servidores, máquinas virtuales e incluso dispositivos móviles gestionados.

A photograph of a man with a beard and a woman sitting at a table, looking at a laptop screen. The man is on the left, wearing a grey t-shirt, and the woman is on the right, wearing a yellow top. The image is overlaid with a semi-transparent teal color. The text 'IMPARTE FORMACIÓN' is written in white, uppercase letters in the lower right quadrant.

IMPARTE  
FORMACIÓN

# IMPARTE FORMACIÓN

Tus empleados deben conocer algo más que las políticas y procedimientos de seguridad de la empresa. También tienen que entender por qué son necesarios. Esto significa **invertir en la concienciación y educación en materia de seguridad**, que suele ser la medida de seguridad más eficaz que se puede aplicar.

Trabajando con tu personal, puedes concienciarlo sobre temas como el correo electrónico de phishing. Un estudio demostró que el 43% de los empleados ni siquiera están seguros de lo que es un ataque de phishing<sup>2</sup>.

Por lo tanto, prepara una formación periódica para tus empleados, por ejemplo, un concurso de phishing, para enseñarles qué técnicas utilizan los ciberdelincuentes. Haz que la concienciación sobre ciberseguridad forme parte del proceso de incorporación y proporciona consejos de seguridad en una página de la intranet.

Asegúrate de formar a todos los que utilizan tus sistemas, incluidos los ejecutivos, los proveedores y los distribuidores. Y **recuerda que las infracciones de las políticas de seguridad deben tener consecuencias**. No hacer cumplir las políticas perjudica todo el esfuerzo de seguridad.

La **formación online gratuita de ESET sobre ciberseguridad** es una forma fácil y eficaz de educar a tu personal. Se tarda menos de 60 minutos en completarla y cubre temas que van desde el phishing y las políticas de contraseñas hasta la seguridad en el lugar de trabajo remoto.

El **69%**  
de las empresas  
sufrieron una  
amenaza interna, a  
pesar de las medidas  
preventivas<sup>3</sup>



SIGUE EVALUANDO,  
AUDITANDO Y  
PROBANDO

# SIGUE EVALUANDO, AUDITANDO Y PROBANDO

La ciberseguridad para cualquier empresa, grande o pequeña, es un proceso continuo, no un proyecto único. Debes planificar **la reevaluación de tu seguridad de forma periódica**, al menos una vez al año.

Es posible que tengas que actualizar tus políticas y controles de seguridad más de una vez al año en función de los cambios que se produzcan en la empresa, como las **nuevas relaciones con los proveedores, los nuevos proyectos, las nuevas contrataciones o la salida de empleados** (asegúrate de que todo el acceso al sistema se revoque cuando alguien deje la empresa). Considera la posibilidad de contratar a un consultor externo para que realice una prueba de infiltración y una auditoría de seguridad para averiguar dónde están tus puntos débiles y resolverlos.

La actual ola de ciberdelincuencia no va a terminar pronto, por lo que es necesario hacer un esfuerzo continuo de buena fe para proteger los datos y los sistemas que son la esencia de la pequeña empresa de hoy en día.

Para estar al día sobre las nuevas amenazas, revisa regularmente las noticias sobre seguridad suscribiéndote a sitios web como:

**[WeLiveSecurity.com](http://WeLiveSecurity.com)**

**[DataSecurityGuide.eset.com](http://DataSecurityGuide.eset.com)**





Durante más de 30 años, ESET® ha desarrollado software de seguridad líder en el sector para empresas y usuarios de todo el mundo. Con soluciones de seguridad que van desde la defensa de equipos y móviles hasta el cifrado y la autenticación de dos factores, los productos de alto rendimiento y fáciles de usar de ESET ofrecen a los usuarios y a las empresas la tranquilidad de disfrutar de todo el potencial de su tecnología. ESET protege y supervisa de forma discreta las 24 horas del día, actualizando las defensas en tiempo real para mantener a los usuarios seguros y a las empresas en funcionamiento sin interrupciones. Para más información, visita [www.eset.es](http://www.eset.es).

