



En la actualidad, la **ciberseguridad en pymes** se ha convertido en un aspecto esencial para garantizar la continuidad del negocio. La digitalización de procesos y la dependencia de la tecnología hacen que incluso las empresas más pequeñas estén expuestas a amenazas constantes que pueden comprometer datos sensibles de clientes, empleados y proveedores.

Aunque muchas pymes no cuentan con departamentos especializados, existen medidas asequibles y efectivas que permiten **proteger la información** sin necesidad de grandes recursos ni conocimientos técnicos avanzados.

## Contenidos



- ¿Por qué la ciberseguridad es clave en las pequeñas empresas?
- Medidas esenciales para proteger tu empresa
- Protección de accesos y dispositivos
- La importancia de la formación del personal
- Prepararse para responder ante incidentes
- Beneficios de reforzar la ciberseguridad en pymes
- Conclusión

## **¿Por qué la ciberseguridad es clave en las pequeñas empresas?**

La ciberseguridad es el conjunto de prácticas y herramientas orientadas a proteger sistemas, redes y datos frente a ataques digitales. Las pymes, por su tamaño, suelen ser percibidas como objetivos fáciles, pero los riesgos son tan reales como en las grandes compañías: **malware, phishing, ransomware o ataques que interrumpen servicios críticos.**

La buena noticia es que dar los primeros pasos hacia una protección eficaz no es

complicado. Aplicar medidas básicas marca una diferencia importante y permite construir una estrategia de seguridad más sólida con el tiempo.

## GUÍA RÁPIDA PARA EMPRESAS

# CIBERSEGURIDAD



Implementa políticas de **CONTRASEÑAS SEGURAS** y exige renovarlas periódicamente

**FORMA A LOS EMPLEADOS** para reconocer ataques como phishing, malware o enlaces fraudulentos



Asegúrate de **ACTUALIZAR SISTEMAS Y SOFTWARE** para evitar vulnerabilidades

**PROTEGE ACCESOS** a sistemas críticos utilizando autenticación en dos factores (2FA)



**PROTEGE TU RED** configurando firewalls, segmentando redes y evitando redes Wi-Fi públicas

Realiza **COPIAS DE SEGURIDAD** automáticas y almacénalas en ubicaciones seguras fuera de la red



ILUSTRE COLEGIO  
OFICIAL DE GESTORES  
ADMINISTRATIVOS  
DE MADRID

## Medidas esenciales para proteger tu empresa

La implementación de la ciberseguridad en una pyme puede abordarse por fases. Entre las acciones prioritarias destacan:

- **Copias de seguridad automáticas** para recuperar datos en caso de incidente.
- **Cifrado de dispositivos** y activación de actualizaciones periódicas.
- **Antivirus y firewalls** como primera línea de defensa.

Estas medidas reducen vulnerabilidades comunes y garantizan que la información esté protegida desde el inicio.

## Protección de accesos y dispositivos

Una vez cubiertas las bases, es fundamental reforzar la seguridad diaria del negocio. Para ello conviene:

- Almacenar información sensible en sistemas seguros.
- Limitar el uso de dispositivos personales para tareas profesionales.
- Aplicar **autenticación multifactor** en accesos críticos.
- Proteger la red Wi-Fi y restringir el acceso físico a los equipos.

Con estas prácticas se evita que terceros no autorizados accedan a la información o a los sistemas de la empresa.

## La importancia de la formación del personal

El factor humano es uno de los eslabones más débiles en materia de seguridad digital. Capacitar a los empleados en **identificación de intentos de phishing**, uso responsable de contraseñas y cumplimiento de políticas de seguridad es esencial para reducir riesgos. Además, realizar auditorías internas periódicas ayuda a detectar fallos antes de que se conviertan en problemas graves.

## Prepararse para responder ante incidentes

Ningún sistema es infalible. Por eso, las empresas deben contar con un **plan de**

**actuación frente a ciberataques**, que incluya protocolos de respuesta rápida y procedimientos de recuperación de datos. De este modo, se minimiza el impacto de cualquier brecha de seguridad.

## **Beneficios de reforzar la ciberseguridad en pymes**

Invertir en ciberseguridad no solo protege la información y sistemas de la empresa, también ofrece ventajas estratégicas:

- **Garantiza la continuidad del negocio** frente a incidentes digitales.
- **Refuerza la confianza de clientes y colaboradores** al demostrar compromiso con la protección de datos.
- Ayuda a cumplir con la normativa vigente, como el **RGPD y la LOPD**, evitando sanciones.
- Contribuye a la reputación y credibilidad de la empresa.

## **Conclusión**

La **ciberseguridad en las empresas** es alcanzable a través de un enfoque progresivo y adaptado a cada negocio. Con medidas económicas y efectivas —desde la protección básica de datos hasta la formación del personal y la preparación ante incidentes—, cualquier empresa puede dar pasos firmes hacia un entorno digital seguro.

Además, los gestores administrativos pueden orientar a las pymes en la modernización de sus procesos, aprovechando iniciativas como el **Kit Digital** para implementar soluciones tecnológicas y mejorar la protección de su actividad.