Acelera pyme

Ciberseguridad para pymes y autónomos: protege tu negocio en el mundo digital y ve un paso por delante

"Una manera de hacer Europa"
Fondo Europeo de Desarrollo Regional

Financiado por la Unión Europea NextGenerationEU

red.es

Plan de Recuperación, Transformación y Resiliencia

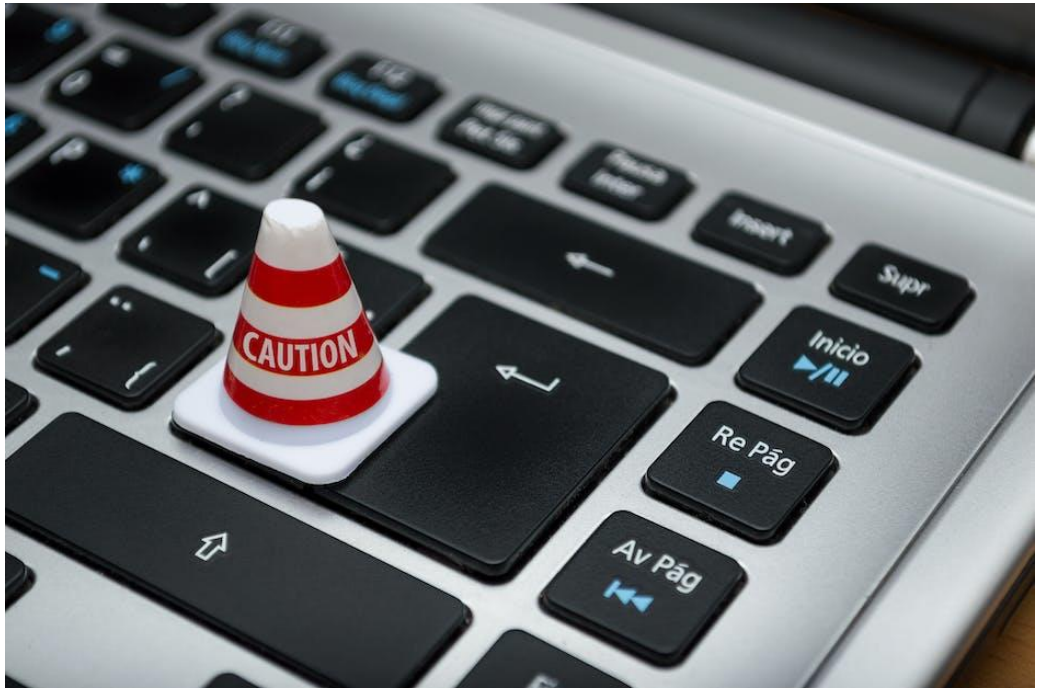
KIT DIGITAL

España | digital 2026

Índice

Introducción

La **ciberseguridad** se ha convertido en una **preocupación creciente** en el mundo empresarial y para la sociedad en general. Los ataques informáticos representan **una amenaza real** que puede poner en peligro la **seguridad de los datos**, la **reputación** y generar **pérdidas económicas** significativas.



Con la creciente digitalización, las **pymes y** los **autónomos** se han vuelto más **vulnerables** a estos ataques, por lo que es **fundamental que estén preparados** y cuenten con **medidas de ciberseguridad adecuadas**.

La concienciación en el ámbito de la ciberseguridad

> El **proceso de concienciación** en el ámbito de la ciberseguridad es algo que puede comenzar **llevando a cabo diversas acciones** como, por ejemplo, las que se enumeran a continuación:

Establecer políticas de ciberseguridad claramente establecidas y comunicarlas de forma eficaz y regular.

Informar de los riesgos con casos reales para ilustrar las consecuencias de la falta de concienciación y conocimiento de ciberseguridad.

Formar y capacitar a los empleados de la pyme con el objetivo de que conozcan los riesgos más comunes y cómo evitarlos.

Intercambiar información con otros organismos y asociaciones para prevenir los ataques más comunes o más recientes.

Amenazas más comunes en ciberseguridad

INCIBE - Guía para **prevenir a diferentes ataques** y **cómo actuar:**

1. Fugas de información
2. Ataques de tipo phishing
3. Fraude del CEO (spear phishing)
4. Fraude de RR.HH.
5. Sextorsión
6. Ataques contra la página web corporativa
7. Ransomware
8. Fraude del falso soporte de Microsoft
9. Campañas de correos electrónicos con malware
10. Ataques de denegación de servicio (DoS)
11. Ataques de adware
12. Ataque de suplantación de proveedores

Protección de datos y consejos prácticos para la implementación de la ciberseguridad

> **Datos susceptibles de ser robados** por ciberdelincuentes :

INFORMACIÓN CORPORATIVA CONFIDENCIAL O PRIVILEGIADA

INFORMACIÓN DE CLIENTES

INFORMACIÓN DE PROVEEDORES

INFORMACIÓN DE EMPLEADOS

CONTRASEÑAS

Protección de datos y consejos prácticos para la implementación de la ciberseguridad

Acelera pyme

PAUTAS BÁSICAS

1. Utilizar **contraseñas** únicas
2. Identificación **multi-factor**
3. Emplear un **firewall**
4. Sistema **operativo actualizado** en todo momento
5. Evitar conectarse a **Wi-Fi público** y activar **VPN**
6. Revisar que los enlaces tienen “**https**”
7. Habilitar la **configuración de privacidad** o aumentarla
8. Precaucionar con la **información personal** que se comparte y dónde
9. Solo descargarse **software verificado** y de fuentes fiables
10. Llevar a cabo de forma regular **copias de seguridad**

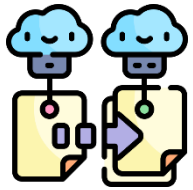
Protección de datos y consejos prácticos para la implementación de la ciberseguridad

Acelera pyme

> Aplicar medidas de ciberseguridad tiene que venir acompañado de una implementación organizada y medida. Por ello, que se proponen las siguientes **estrategias**:

Desarrollar un plan de ciberseguridad

Establecer una respuesta a incidentes



Realizar copias de seguridad regulares

Establecer políticas de seguridad

Implementar medidas de seguridad técnicas

Capacitar y concienciar a los empleados

Mantener el software actualizado

Reducir la huella digital

Herramientas y tecnologías de ciberseguridad

Antivirus

- Bitdefender Antivirus Free
- Avast Free Antivirus

VPN

- Hotspot Shield
- ProtonVPN Free

Firewall

- Windows Defender
- ZoneAlarm
- Comodo Free Firewall

Gestor de contraseñas

- 1Password
- LastPass

Conclusiones

En resumen, **las pymes y los autónomos deben estar preparados** para hacer frente a las **amenazas de ciberseguridad**. La concienciación, la comprensión de las amenazas comunes, la protección de datos y la implementación de medidas de seguridad adecuadas son aspectos fundamentales para minimizar los riesgos.

La ciberseguridad **debe ser una prioridad** para todas las empresas, ya que los ataques **pueden tener graves consecuencias** tanto en términos de seguridad como económicos.

Acelera pyme

"Una manera de hacer Europa"

Fondo Europeo de Desarrollo Regional

Financiado por la Unión Europea NextGenerationEU

Gobierno de España · Vicepresidencia Primera del Gobierno · Ministerio de Asuntos Económicos y Transformación Digital · Secretaría de Estado de Digitalización e Inteligencia Artificial

red.es

Plan de Recuperación, Transformación y Resiliencia

KIT DIGITAL

España | digital 2026