

Los 5 errores de seguridad que no debes cometer

Gastar miles de euros en alarmas, detectores de humo y cámaras es normal, pero pocos se preocupan por proteger sitios web y empresas de ataques externos. Con el número creciente de hackers activos en la red conviene saber qué errores evitar.

Cinco errores frecuentes

- Pensar que se es demasiado pequeño: muchas PYMEs se creen inmunes porque no se consideran un objetivo interesante. En realidad, una parte relevante de los ataques afecta precisamente a empresas pequeñas y medianas.
- Usar contraseñas débiles o por defecto: contraseñas como "1234" o "p4ssw0rd", sin autenticación multifactor, invitan a acceder a los datos empresariales.
- Exponer vulnerabilidades: SQL Injection y XSS son vulnerabilidades comunes en aplicaciones web y pueden causar daños graves, sobre todo cuando no existe seguridad interna.

- No educar a los usuarios: correo no seguro, redes no fiables y credenciales mal gestionadas exponen a la empresa. Formar a las personas reduce el riesgo diario.
- No actualizar los sistemas: cada día se descubren nuevas vulnerabilidades. Aplicaciones y sistemas actualizados reducen el riesgo de ataques con técnicas conocidas.

La pregunta que debes hacerte

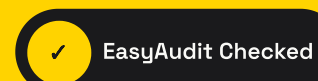
¿Crees que tu empresa es segura? Tus proveedores no se ocupan de tu seguridad: debes interesarte tú.

EasyAudit simula un atacante externo y te permite entender tu nivel de seguridad, ayudándote a identificar fallos y corregirlos.

¿Quieres saber si tu empresa está realmente protegida?

EasyAudit verifica aplicaciones, infraestructuras y plataformas E-Commerce con una auditoría clara, concreta y pensada para transformar riesgos técnicos en decisiones simples.

Solicita una auditoría en easyaudit.es



La señal visible de un compromiso serio con la seguridad.