CyberSecurity Group

10 preguntas para saber si tu empresa está expuesta

Un chequeo rápido, sin tecnicismos, para identificar los puntos ciegos más comunes en ciberseguridad antes de que se conviertan en un incidente.

1. Accesos — ¿Sabes exactamente quién tiene acceso a tus sistemas críticos y desde cuándo, incluyendo ex empleados y proveedores externos?

2. Contraseñas — ¿Tu empresa usa autenticación de múltiples factores (MFA) en el correo corporativo y en los sistemas administrativos?

3. Respaldo — ¿Cuándo fue la última vez que probaron restaurar un respaldo real, no solo que se generó el archivo?

4. Parches — ¿Existe un proceso definido y con plazos para aplicar actualizaciones de seguridad críticas?

5. Terceros — ¿Conocen qué proveedores externos tienen acceso a datos sensibles de la empresa o de clientes?

6. Phishing — ¿El equipo ha recibido capacitación o simulacros de phishing en el último año?

7. Incidentes — ¿Existe un plan escrito de qué hacer en las primeras 24 horas tras detectar un incidente?

8. Dispositivos — ¿Los dispositivos móviles y laptops del equipo tienen cifrado de disco activado?

9. Desarrollo — Si desarrollan software propio, ¿se revisa el código en busca de vulnerabilidades antes de salir a producción?

10. Cumplimiento — ¿Saben qué normativas o marcos (ISO 27001, Ley Marco de Ciberseguridad, etc.) les aplican como organización?

Cómo leer tus resultados

Si respondiste “no” o “no estoy seguro” a tres o más preguntas, es un buen momento para una evaluación formal — muchas veces los riesgos más costosos no son técnicamente sofisticados, sino puntos básicos que nadie revisó a tiempo.