CHECKLIST DE PREPARACIÓN EN CIBERSEGURIDAD

Este checklist permite evaluar qué tan preparada está la empresa frente a un ataque real, identificando brechas en competencias TI, respuesta a incidentes y madurez en ciberseguridad.

Versión 1.0 - Junio de 2026

1. Nivel de competencias del equipo de TI

Elemento	Cumple	No Cumple
• El equipo identifica amenazas críticas como phishing, ransomware, malware y robo de credenciales.	☐	☐
• Existen responsables definidos para gestionar alertas, incidentes y controles de seguridad.	☐	☐
• Los activos críticos están identificados según su impacto en la operación del negocio.	☐	☐
• Los accesos sensibles y cuentas privilegiadas están identificados y bajo control.	☐	☐
• El equipo mantiene conocimientos actualizados sobre vulnerabilidades, parches y protección de sistemas.	☐	☐
• Se realizan ejercicios técnicos para mejorar la detección y respuesta ante incidentes.	☐	☐

2. Capacidad de respuesta frente a un ataque real

Elemento	Cumple	No Cumple
• Existe un plan de respuesta ante incidentes documentado, actualizado y conocido por las áreas clave.	☐	☐
• La empresa tiene un canal claro para reportar incidentes, alertas o comportamientos sospechosos.	☐	☐
• Hay una cadena de escalamiento definida para actuar rápido ante incidentes críticos.	☐	☐
• Existen procedimientos para contener, analizar y recuperar sistemas afectados por un ataque.	☐	☐
• Los respaldos están actualizados, protegidos y han sido probados recientemente.	☐	☐
• Los incidentes se documentan con evidencias, decisiones tomadas y lecciones aprendidas.	☐	☐

3. Nivel de madurez en ciberseguridad

Elemento	Cumple	No Cumple
• La empresa cuenta con políticas de ciberseguridad documentadas, vigentes y comunicadas.	☐	☐
• Existe un inventario actualizado de activos, sistemas, usuarios y servicios expuestos.	☐	☐
• Los accesos se gestionan bajo el principio de mínimo privilegio y revisión periódica.	☐	☐
• La autenticación multifactor está activa en sistemas críticos y accesos remotos.	☐	☐
• Los parches de seguridad se aplican de forma periódica, priorizando riesgos críticos.	☐	☐
• Los controles se alinean con buenas prácticas como ISO 27001, NIST, CIS Controls o normativa aplicable.	☐	☐

4. Resultado de la Autoevaluación

Sume la cantidad total de elementos marcados como Cumple

Resultado	Nivel de preparación
0 a 8 cumplimientos	**Preparación baja**
9 a 16 cumplimientos	**Preparación intermedia**
17 a 22 cumplimientos	**Preparación avanzada**
23 a 25 cumplimientos	**Preparación sólida**

5. Interpretación del Resultado

Preparación baja:

- Existen brechas críticas que pueden afectar la detección, respuesta o recuperación frente a un ataque.

Preparación intermedia:

- La empresa cuenta con avances, pero aún mantiene puntos débiles que deben priorizarse.

Preparación avanzada:

- Existe una base sólida, aunque es necesario validar controles, procesos y capacidad de respuesta.

Preparación sólida:

- La empresa demuestra una buena preparación, pero debe revisar sus controles de forma continua.

6. Conclusión y Plan de Acción

Acción Prioritaria		Responsable	Plazo estimado
Revisar puntos “No Cumple”.	✓	**TI / Seguridad**	**15 días**
Definir responsables y escalamiento.	✓	**Gerencia / TI**	**30 días**
Validar respaldos y accesos críticos.	✓	**TI / Infraestructura**	**45 días**
Evaluar brechas y vulnerabilidades.	✓	**TI / Seguridad**	**60 días**
Realizar simulacro de incidente.	✓	**TI / Seguridad**	**75 días**
Crear plan de mejora continua.	✓	**Gerencia / TI**	**90 días**

RECOMENDACIÓN:

Aborda primero los puntos marcados como **No Cumple** en accesos, respaldos, monitoreo, respuesta ante incidentes y competencias del equipo de TI.