Checklist: ¿Tu empresa está lista para resistir un ataque de phishing?

Evalúa tu nivel de preparación y fortalece tu primera línea de defensa con esta herramienta práctica.

Ponemos a su disposición

Una guía para líderes de TI, cumplimiento, recursos humanos y seguridad corporativa.
Desarrollado por Guardianes del Golfo.

¿Por qué necesitas este checklist?

El phishing sigue siendo una de las técnicas más efectivas para vulnerar organizaciones.
Aprovecha el error humano, el descuido y la falta de conciencia.
Este checklist te permitirá identificar si tu empresa cuenta con las políticas, herramientas y cultura necesarias para detectar, prevenir y responder ante un intento de phishing.

"Lo que no se evalúa, no se puede mejorar."

¿Cómo usar este checklist?

- Lee cada afirmación y marca ✓ si aplica completamente a tu organización.
- Si la respuesta es "no" o "en parte", es una **área de oportunidad.**

- Al final, haz un conteo total de respuestas afirmativas para obtener tu nivel de preparación.

!!! Este documento no sustituye una auditoría formal, pero es un excelente punto de partida para tomar acción !!!

Evaluación de preparación ante phishing

---

1. Concientización del personal

□ ¿El equipo ha recibido capacitación sobre phishing en los últimos 6 meses?
□ ¿Saben identificar enlaces, remitentes y archivos sospechosos?
□ ¿Tienen claro qué hacer si detectan un intento de phishing?
□ ¿Se realizan simulaciones periódicas con retroalimentación?

2. Herramientas y controles técnicos

□ ¿Usamos filtros de correo para bloquear mensajes maliciosos?
□ ¿Hay advertencias visibles para correos externos o peligrosos?
□ ¿Los empleados pueden ver el dominio real de los remitentes?

3. Políticas internas y cultura organizacional

□ ¿Existe una política clara de uso del correo corporativo?
□ ¿Tenemos definida una política de contraseñas seguras (2FA, rotación)?
□ ¿Contamos con procedimientos formales para reportar incidentes?

4. Respuesta ante incidentes

□ ¿El personal sabe cómo y a quién reportar un intento de phishing?
□ ¿Tenemos un plan básico de respuesta para contener el daño?
□ ¿Se hace análisis posterior a incidentes para evitar repetición?

5. Monitoreo y mejora continua

□ ¿Medimos los resultados de las campañas de concientización?
□ ¿Tenemos responsables designados para la seguridad de la información?
□ ¿Revisamos y actualizamos regularmente nuestras medidas de protección?

Interpreta tu nivel de preparación

Haz el conteo total de checks y compáralo con la siguiente escala:

Respuestas	Nivel de preparación	Recomendación
13-15	Alto	Mantén buenas prácticas y refuerza la cultura continuamente.
9-12	Medio	Existen brechas importantes. Prioriza acciones correctivas.
8 o menos	**Bajo**	**Tu organización está en riesgo. Se requiere intervención urgente.**

¿Qué sigue después de este diagnóstico?

Este checklist es el primer paso. Si detectaste áreas de oportunidad, estás a tiempo de actuar.
Nuestro equipo puede ayudarte a diseñar una estrategia de concientización efectiva, alineada a los riesgos reales de tu empresa.

Desarrollado por Guardianes del Golfo

Web	Teléfono	Correo
guardianesdelgolfo.net	+52 22-95-91-22-46	info@guardianesdelgolfo.com