CHECKLIST PRÁCTICO

SEÑALES DE RIESGO EN INFRAESTRUCTURA

Este checklist es una herramienta de apoyo para **identificar señales tempranas de riesgo** en infraestructura tecnológica, revisar controles existentes y priorizar acciones antes de que una **brecha o debilidad pueda escalar**

Versión 1.0 - Abril 2026

1. Exposición externa

Elemento	Cumple	No Cumple
• Activos públicos con inventario actualizado.	☐	☐
• Servicios expuestos en Internet con justificación vigente.	☐	☐
• Paneles de administración restringidos desde redes externas.	☐	☐
• Dominios, subdominios y certificados con responsable definido.	☐	☐

2. Identidad y accesos

Elemento	Cumple	No Cumple
• Cuentas privilegiadas con MFA o control adicional.	☐	☐
• Usuarios activos alineados a su rol actual.	☐	☐

• Accesos individuales con trazabilidad clara.	☐	☐
• VPN, RDP o SSH con restricción de origen.	☐	☐

3. Parches y configuración

Elemento	Cumple	No Cumple
• Servidores con parches críticos aplicados.	☐	☐
• Sistemas y servicios sin configuraciones por defecto.	☐	☐
• Reglas de firewall vigentes y con responsable asignado.	☐	☐
• Cambios productivos con validación técnica y plan de reversa.	☐	☐

4. Monitoreo y respuesta

Elemento	Cumple	No Cumple
• Logs completos y centralizados.	☐	☐
• Alertas repetidas con cierre y causa raíz documentada.	☐	☐
• Activos críticos con monitoreo de disponibilidad y seguridad.	☐	☐
• Evidencia suficiente para auditoría o investigación.	☐	☐

5. Continuidad y terceros

Elemento	Cumple	No Cumple
• Respaldos probados con restauración real.	☐	☐
• Proveedores críticos con revisión de accesos y responsabilidades.	☐	☐

- Credenciales de integración con rotación definida. ☐ ☐
- Activos clasificados según criticidad. ☐ ☐
- Simulacros de respuesta a incidentes realizados ☐ ☐

6. Señales que requieren atención prioritaria

Elemento	Cumple	No Cumple
Servicio crítico expuesto a Internet sin justificación.	☐	☐
Cuenta privilegiada sin MFA o con acceso compartido.	☐	☐
Respaldos sin prueba reciente de restauración.	☐	☐
Alertas repetidas sin causa raíz documentada.	☐	☐
Proveedor con accesos activos sin revisión.	☐	☐
Inventario incompleto de activos públicos.	☐	☐

7. Conclusión y Plan de Acción

Acción Prioritaria	Responsable	Plazo estimado
Revisar activos públicos sin inventario actualizado ✓	**Infraestructura**	**30 días**
Validar cuentas privilegiadas y accesos críticos ✓	**Seguridad / TI**	**45 días**
Probar respaldos mediante restauración real ✓	**Infraestructura**	**60 días**
Documentar causa raíz de alertas repetidas ✓	**SOC / Seguridad**	**60 días**
Documentar causa raíz de alertas repetidas ✓	**Seguridad / TI**	**90 días**

RECOMENDACIÓN:

Abordar primero los puntos marcados como **No Cumple** en áreas críticas como exposición externa, accesos privilegiados, monitoreo, respaldos y terceros.

- Este checklist sirve como línea base para **identificar debilidades**, **asignar responsables** y **priorizar acciones de mejora**.
- Se recomienda revisarlo periódicamente o ante cambios relevantes en la infraestructura, accesos, servicios expuestos o proveedores críticos.

I3G Ciberseguridad

Validamos tus defensas con una mirada práctica, clara y orientada al riesgo