// DIAGNÓSTICO EJECUTIVO · 2026

Checklist diagnóstico

¿En qué nivel de madurez de inventario está tu organización?

Para CISOs, CIOs, gerentes de TI / riesgo / cumplimiento que necesitan saber, antes de invertir en EDR, SIEM o cualquier capa de protección, **si tienen un inventario auditable de lo que están protegiendo**.

Este checklist es **auto-administrado en 8 minutos**. Responde 20 preguntas Sí/No, suma los puntos y descubre tu nivel de madurez en una escala 0–4 alineada con ISO/IEC 27001:2022 A.5.9, NIST CSF ID.AM, CIS Controls #1 y la Ley 21.663 chilena.

8 min	20 preguntas	5 niveles	4 frameworks
Auto-administrado	Sí / No	Madurez 0–4	ISO · NIST · CIS · Ley 21.663

Instrucciones

1. Lee cada pregunta y marca **Sí** solo si tu organización la cumple **hoy y de forma sistemática** (no "estamos en eso").
2. Suma 1 punto por cada Sí. Anota el total al final de cada bloque.
3. Suma los 4 bloques y consulta la tabla de la página 3 para identificar tu nivel.
4. En la página 4 encontrarás el plan de acción priorizado para tu nivel.

Esta herramienta es una versión simplificada del Diagnóstico GAP Multi-Norma que TTPSEC ejecuta en 15–21 días con evidencia auditable, NDA y propuesta formal de remediación. Solicita el diagnóstico completo en www.ttpsec.cl

Las 20 preguntas

// Marca Sí solo si tu organización cumple hoy y de forma sistemática.

A · Gobierno del inventario (5 puntos)

1.	¿Existe un único inventario consolidado de activos tecnológicos en toda la organización?	Sí ■	No ■
2.	¿Tiene un responsable nombrado por escrito (dueño del registro)?	Sí ■	No ■
3.	¿Se reconcilia mensualmente contra el discovery activo?	Sí ■	No ■
4.	¿El delta entre inventario y realidad se reporta al comité de auditoría o directorio?	Sí ■	No ■
5.	¿Cubre el 100% del cómputo (no solo el alcance certificado)?	Sí ■	No ■
	Subtotal bloque (A)		____ / 5

B · Discovery y cobertura (5 puntos)

1.	¿Hay un discovery activo (Lansweeper / Tanium / Qualys / runZero / Axonius) operando hoy?	Sí ■	No ■
2.	¿El discovery cubre on-prem + nube (AWS/Azure/GCP) + SaaS conectado por OAuth?	Sí ■	No ■
3.	¿Se inventarían contenedores, funciones serverless e identidades de servicio?	Sí ■	No ■
4.	¿Se cruza el discovery con el catálogo de licencias y con identidades del IdP?	Sí ■	No ■
5.	¿Existe alerta automática cuando aparece un activo no declarado en el CMDB?	Sí ■	No ■
	Subtotal bloque (B)		____ / 5

C · Ontología y propiedad (5 puntos)

1.	¿Existe definición formal y firmada de "qué es un activo" para tu organización?	Sí ■	No ■
2.	¿Está documentado cuándo nace y cuándo muere un activo (alta / baja)?	Sí ■	No ■
3.	¿Cada activo tiene asignado dueño técnico, funcional y de dato (3 separados)?	Sí ■	No ■
4.	¿Cada activo está cruzado con el servicio de negocio que entrega?	Sí ■	No ■
5.	¿Cada activo tiene clasificación de criticidad (RTO / RPO definidos)?	Sí ■	No ■
	Subtotal bloque (C)		____ / 5

D · Auditoría y consecuencias (5 puntos)

1.	¿El auditor externo recibe el inventario antes de que IT lo "prepare"?	Sí ■	No ■

2.	¿Existe consecuencia contractual para activos no declarados (sin soporte, sin parches)?	Sí ■	No ■
3.	¿El inventario alimenta directamente al SIEM, EDR, vuln scanner y PAM?	Sí ■	No ■
4.	¿Se puede responder "¿qué hay en producción sin EDR?" en menos de 5 minutos?	Sí ■	No ■
5.	¿El CISO o seguridad opera su propio Shadow CMDB independiente de IT?	Sí ■	No ■
	Subtotal bloque (D)		**___ / 5**

TOTAL (suma de los 4 bloques) ___ / 20

Tu nivel de madurez

// Suma del total ■ Nivel 0 a 4

0–4 pts	Nivel 0 · Excel federado	Riesgo: Crítico

Cada área tiene su propio Excel. Nadie tiene la suma. La superficie de ataque agregada es desconocida. Cualquier inversión en EDR/SIEM opera sobre un mapa parcial.

5–9 pts	Nivel 1 · CMDB instalado, sin alimentar	Riesgo: Alto

Existe un CMDB (ServiceNow / BMC / Cherwell / GLPI). Se pobló una vez. Hoy refleja el pasado. La conciliación no se ejecuta.

10–13 pts	Nivel 2 · Discovery sin gobierno	Riesgo: Medio

Hay un discovery (Lansweeper / Tanium / Qualys). Captura la realidad técnica. No se cruza con servicios, licenciamiento ni propiedad. Datos sin información.

14–17 pts	Nivel 3 · Inventario consolidado, gobernado por IT	Riesgo: Bajo

Existe un inventario único, con dueño técnico, funcional y de dato. Cruzado con servicios. Pero vive en IT — vulnerable a las 6 razones políticas de la resistencia.

18–20 pts	Nivel 4 · Inventario consolidado + Shadow CMDB de seguridad	Riesgo: Controlado

Coexisten dos inventarios: el de IT y el de seguridad. Se reconcilian. Delta reportado al directorio. Consecuencias contractuales activas. Auditor externo consume ambos.

La mayoría de organizaciones latinoamericanas está en Nivel 1 o 2. Una minoría llega a Nivel 3. El Nivel 4 es excepcional y, generalmente, corresponde a entidades reguladas con auditoría sectorial intrusiva (bancos sistémicos, infraestructura crítica supervisada).

Tu plan de 90 días

// Próximo paso según tu nivel actual

■ Si estás en Nivel 0 o 1

• Día 1–30: Levantar inventario base con discovery (Lansweeper o Tanium en piloto)

• Día 31–60: Cruzar con catálogo de licencias y con CMDB existente; identificar delta

• Día 61–90: Definir dueño técnico/funcional/dato por cada activo crítico

• Salida esperada: Nivel 2 estable + alcance para certificación parcial ISO 27001

■ Si estás en Nivel 2

• Día 1–30: Formalizar las 5 preguntas ontológicas (¿qué es un activo?, etc.)

• Día 31–60: Conectar discovery con SIEM/EDR/IdP; producir vista unificada

• Día 61–90: Implementar reporte mensual al comité de auditoría con delta

• Salida esperada: Nivel 3 con gobierno IT formal

■ Si estás en Nivel 3

• Día 1–30: Diseñar arquitectura Shadow CMDB autónomo (Cartography / CAASM)

• Día 31–60: Desplegar consultas críticas (¿qué hay sin EDR?, ¿qué hay sin CMDB?)

• Día 61–90: Formalizar consecuencias contractuales para activos no declarados

• Salida esperada: Nivel 4 con auditoría dual IT + Seguridad

¿Quieres el diagnóstico completo?

El **GAP Assessment Multi-Norma** de TTPSEC evalúa tu organización contra **7 frameworks simultáneos** (ISO 27001, NIST CSF, IEC 62443, Ley 21.663, ANCI, ENS, CIS Controls v8) en **15–21 días**, con NDA, modalidad remota y propuesta formal en 48 horas.

→ **www.ttpsec.cl** · **contacto@ttpsec.com**

Sobre TTPSEC · Centro de Excelencia en Ciberseguridad Industrial. Cumplimiento Ley 21.663 / ANCI / OIV · OT/ICS · IT · IA · Chile + LATAM.