

Auditoría de ciberseguridad para empresas

Ejemplo simplificado de cómo Tecnidom presenta un hallazgo técnico con contexto, evidencia, prioridad, remediación y criterio de verificación.

Resumen ejecutivo

Este documento es una muestra comercial y utiliza exclusivamente datos ficticios. No corresponde a una auditoría real ni contiene información de ningún cliente.

ALCANCE	RESULTADO	PRIORIDAD
Exposición externa autorizada	1 hallazgo de ejemplo	ALTA
Objetivo ficticio: portal.example.test	Evidencia + contexto + acción	Requiere actuación prioritaria

Qué demuestra esta muestra

- El hallazgo no se limita a indicar que existe un puerto o servicio accesible.
- La evidencia técnica se conserva y se relaciona con el activo observado.
- La prioridad se interpreta según exposición, función del activo y controles existentes.
- La recomendación incluye una forma concreta de verificar la corrección.

Hallazgo H-001 · Interfaz de administración expuesta a Internet

Severidad	Activo	Servicio	Estado
ALTA	portal.example.test	TCP/8443 · HTTPS	ABIERTO

EVIDENCIA OBSERVADA

Durante una comprobación externa incluida en el alcance autorizado, el servicio de administración en TCP/8443 respondió desde una red pública. La evidencia conserva objetivo, puerto, protocolo, herramienta y momento de ejecución.

RIESGO

La exposición pública de una interfaz de gestión aumenta la superficie de ataque y facilita el descubrimiento de un servicio que, según el supuesto de esta muestra, no necesita estar disponible para Internet.

IMPACTO

Un intento de acceso, abuso de credenciales o explotación de una vulnerabilidad futura afectaría a un punto de administración del entorno. La criticidad final debe ajustarse al rol real del activo y a los controles de autenticación existentes.

RECOMENDACIÓN PRIORITARIA

Restringir el acceso al servicio mediante VPN, lista de orígenes autorizados o reglas de firewall. Mantener la administración fuera de la exposición pública siempre que el caso de uso lo permita.

CRITERIO DE VERIFICACIÓN

Repetir la comprobación desde una red externa no autorizada. El hallazgo puede considerarse corregido cuando TCP/8443 deja de ser accesible desde Internet y el acceso administrativo continúa disponible por el canal autorizado.

Cómo se convierte el hallazgo en una decisión

1 · DATO TÉCNICO	2 · CONTEXTO	3 · ACCIÓN	4 · VERIFICACIÓN
Servicio accesible en TCP/8443.	Es una interfaz de gestión y no necesita exposición pública.	Restringir por VPN, allowlist o firewall.	Repetir la prueba desde una red externa.

Qué puede contener una entrega AuditCore

Resumen ejecutivo	Estado observado y prioridades para dirección.
Inventario técnico	Hosts, puertos, servicios y tecnologías dentro del alcance.
Hallazgos priorizados	Descripción, riesgo, impacto, evidencia y remediación.
Evidencias	Resultados trazables vinculados a herramientas y comprobaciones.
Plan de mejora	Acciones ordenadas por prioridad y contexto.
Reauditoría	Verificación posterior de las correcciones aplicadas.

Importante: AuditCore es una plataforma propia utilizada por Tecnidom para prestar auditorías de ciberseguridad supervisadas profesionalmente. Alcance, profundidad y técnicas se acuerdan antes de cada trabajo.