Checklist de evidencias para clientes enterprise

Talsoft TS

Checklist de evidencias para clientes enterprise - Talsoft TS

Uso recomendado:
Usar este checklist como punto de partida para ordenar evidencias antes de responder cuestionarios de seguridad, vendor reviews o pedidos contractuales. No reemplaza un diagnostico GAP, una auditoria externa ni una revision legal.

1. Gobierno y ownership

- Responsable interno de seguridad o riesgo definido.
- Lista de owners por dominio: accesos, infraestructura, producto, proveedores, incidentes.
- Registro de decisiones o riesgos aceptados.

2. Politicas y procedimientos

- Politica de seguridad de la informacion.
- Politica de control de accesos.
- Procedimiento de respuesta a incidentes.
- Procedimiento de gestion de cambios.
- Procedimiento de backups y recuperacion.

3. Accesos e identidad

- MFA habilitado en sistemas criticos.
- Lista de usuarios privilegiados.
- Proceso de alta, baja y modificacion de accesos.
- Evidencia de revision periodica de accesos.

4. Vulnerabilidades y PenTest

- Inventario de activos relevantes.
- Evidencia de escaneos o revisiones de vulnerabilidades.
- Registro de hallazgos, severidad, owner y estado.
- Evidencia de remediacion o aceptacion de riesgo.
- PenTest conectado a roadmap si aplica.

5. Backups y continuidad

- Alcance de backups.
- Frecuencia de backup.
- Evidencia de prueba de restauracion.
- Owner del proceso.

6. Incidentes

- Canal interno para reportar incidentes.
- Playbook o procedimiento basico.
- Registro de incidentes o simulacros si existen.

- Contactos internos y externos relevantes.

7. Proveedores
- Lista de proveedores criticos.
- Criterio de evaluacion de proveedores.
- Evidencia contractual o de seguridad disponible.
- Owner de seguimiento.

8. Awareness y personas
- Evidencia de capacitaciones o comunicaciones.
- Registro de participantes si aplica.
- Reglas basicas de phishing, passwords, datos y herramientas de IA.

9. Evidencia minima reutilizable
- Carpeta por dominio.
- Fecha de ultima actualizacion.
- Owner de cada evidencia.
- Notas sobre brechas pendientes.

10. Lo que no conviene hacer
- No inventar controles.
- No prometer certificaciones, aprobaciones o ausencia de incidentes.
- No compartir arquitectura, credenciales, vendors sensibles o datos privados sin criterio.
- No responder "si" cuando el control existe solo parcialmente.

Siguiente paso sugerido:
Si faltan evidencias, owners o prioridades, conviene realizar un Initial GAP + Roadmap para ordenar brechas, riesgos y plan de accion.