HodeiShield · Evaluación de plataformas de riesgo de terceros

Checklist de evaluación de plataformas TPRM por sector

Marca cada punto durante la demo con tus propios proveedores y anota lo que la herramienta no hace.

Criterios que valen para cualquier sector

- [ ] Inventario de terceros con responsable interno, criticidad, datos del contrato y subcontratistas.
- [ ] Evidencia con responsable, fecha de validez y estado, y que la caducada deje de contar.
- [ ] Cómo se obtiene la información del proveedor: cuestionario, documentos, escaneo externo, SBOM. Cada vía mide algo distinto.
- [ ] Cómo se calcula la puntuación o el riesgo: entradas visibles, método documentado y estimaciones marcadas como tales.
- [ ] Registro de cambios, exportación de tus datos y API, para poder salir de la herramienta.
- [ ] Dónde se alojan los datos, qué subencargados participan y qué no hace la plataforma. Ninguna te hace cumplir por sí sola.

DORA: entidades financieras de la UE

- [ ] Registro con LEI, jurisdicción, función que apoya y criticidad por proveedor y por contrato.
- [ ] Exportación en el formato de las plantillas oficiales (las guías de los supervisores citan paquetes xBRL-CSV), y que la presentación por el canal oficial siga siendo tuya.
- [ ] Seguimiento por contrato de plan de salida, derecho de auditoría y cadena de subcontratación.
- [ ] Vista de concentración: cuántas funciones dependen de un mismo proveedor.

Fuente: Reglamento (UE) 2022/2554 (DORA), artículos 28 a 31, en EUR-Lex `https://eur-lex.europa.eu/eli/reg/2022/2554/oj` Reglamento de Ejecución (UE) 2024/2956, plantillas del registro de información, en EUR-Lex `https://eur-lex.europa.eu/eli/reg_impl/2024/2956/oj`

NIS2: entidades esenciales e importantes de la UE

- [ ] Evaluación por proveedor con vulnerabilidades y prácticas de seguridad, no solo un cuestionario genérico.
- [ ] Cláusulas de notificación de incidentes del proveedor hacia ti, con seguimiento del plazo.
- [ ] Informes que el órgano de dirección pueda aprobar y revisar.
- [ ] Gestión de incidentes con los plazos del artículo 23: 24 horas, 72 horas y un mes.

Fuente: Directiva (UE) 2022/2555 (NIS2), artículos 20, 21 y 23, en EUR-Lex https://eur-lex.europa.eu/eli/dir/2022/2555/oj
Reglamento de Ejecución (UE) 2024/2690, requisitos técnicos y metodológicos, en EUR-Lex https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj

---

ENS: sector público español y sus proveedores

- [ ] Que distinga la categoría del sistema (básica, media, alta) y muestre qué medidas op.ext aplican.
- [ ] Acuerdos de nivel de servicio por proveedor y medición periódica de su cumplimiento.
- [ ] Análisis de impacto y riesgo por incidente originado en la cadena de suministro, con medidas de contención.
- [ ] Estado de conformidad ENS del propio proveedor cuando presta servicio a una entidad pública.

Fuente: Real Decreto 311/2022 (ENS), artículo 2 y anexo II, medidas op.ext, en el BOE https://www.boe.es/buscar/act.php?id=BOE-A-2022-7191

HIPAA: sanidad en EE. UU. y asociados de negocio

- [ ] Marca de qué terceros tocan información de salud y estado del contrato de asociado de negocio de cada uno, con fechas.
- [ ] Registro de subcontratistas del asociado y de sus garantías.
- [ ] Seguimiento de las cláusulas de notificación de brechas y del plazo de 60 días.
- [ ] Si la propia plataforma va a almacenar información de salud, es asociado de negocio: pide el contrato antes de cargar datos.

Fuente: 45 CFR 164.308(b), contratos con asociados de negocio, en eCFR https://www.ecfr.gov/current/title-45/section-164.308
45 CFR 164.314(a), contratos de asociados de negocio (Regla de Seguridad), en eCFR https://www.ecfr.gov/current/title-45/section-164.314
45 CFR 164.502(e), divulgaciones a asociados de negocio, en eCFR https://www.ecfr.gov/current/title-45/section-164.502
45 CFR 164.504(e), contenido de los contratos de asociado de negocio, en eCFR https://www.ecfr.gov/current/title-45/section-164.504
45 CFR 164.410, notificación del asociado de negocio, en eCFR https://www.ecfr.gov/current/title-45/section-164.410

CMMC 2.0: cadena de suministro de defensa de EE. UU.

- [ ] Campo por proveedor con el tipo de información que maneja (FCI o CUI) y el nivel CMMC que se le exige.
- [ ] Evidencia de que has trasladado los requisitos en el contrato (flow-down).
- [ ] Estado de cada subcontratista frente al nivel exigido, con fecha de la última evidencia.
- [ ] Si vas a cargar CUI en la herramienta, que su alojamiento cumpla el requisito de nube del 170.16(c).

Fuente: 32 CFR 170.23, aplicación a subcontratistas, en eCFR https://www.ecfr.gov/current/title-32/section-170.23
32 CFR parte 170 (programa CMMC), en eCFR https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170

SAMA y ECC de la NCA: sector financiero y nacional de Arabia Saudí

- [ ] Que la biblioteca de marcos incluya SAMA y ECC y que indique la edición (la que hemos consultado es ECC-2:2024).
- [ ] Inventario de terceros con acceso a sistemas o datos y cláusulas contractuales por proveedor.
- [ ] Marca de los proveedores de externalización y de nube, que tienen subdominio propio en SAMA.
- [ ] Evidencia por control, con responsable y fecha, para responder a la entidad supervisora.

Fuente: Marco de Ciberseguridad de SAMA, dominio 3.4 «Third Party Cyber Security», en el Rulebook de SAMA https://rulebook.sama.gov.sa/en/34-third-party-cyber-security-0
Controles Esenciales de Ciberseguridad (ECC-2:2024), dominio 4, de la NCA https://cdn.nca.gov.sa/api/files/public/upload/da829b21-c4ef-4a6e-9f6e-82690d612ee9_ECC-2-2024-.pdf

---

Notas