

PRÁCTICAS ESTANDARIZADAS DE CONTRATACIÓN SEGURA Y DIRECTRICES DE CIBERSEGURIDAD PARA LA CADENA DE SUMINISTRO PARA LA REGIÓN DE AMÉRICA LATINA Y EL CARIBE (ALC)

Prácticas estandarizadas de **LAC4 and EU CyberNet** por **Predrag Tasevski & Florian Göhler**

Alineado con NIS2 · Reglamento de Ciberresiliencia (CRA) de la UE · Buenas Prácticas de ENISA para la Ciberseguridad de la Cadena de Suministro (2023) · Panorama de Amenazas de ENISA sobre Ataques a la Cadena de Suministro (2021) · Plantilla SCRM para Proveedores de CISA · ISO/IEC 27036 · NIST SP 800-161 Rev. 1 · RTS de DORA · Caja de Herramientas de la UE para la Cadena de Suministro de TIC



ity, cybersecurity
technology security
he protection of
s and networks
disclosure,
ge to their
ere, or electronic
from
r misdirection of the
vide.[1]

Computer security, cyber
or information technology
(IT security) is the protec
computer systems and ne
from information disclosure
theft of or damage to the
hardware, software, or st
data, as well as from
the disruption or misdire
services they provide.[1]

Barsecurity
cy security
ection of the
[1]

2 3 1 5 1 2 1 3 2 5 6 1 1 2 1
2 1 3 2 3 1 5 6 2 1 3 1 2



Prólogo-----	4
1. Resumen Ejecutivo-----	6
2. Introducción-----	8
2.1 Contexto y objetivos -----	8
2.2 Alcance y destinatarios -----	8
2.3 Cómo utilizar este documento-----	8
3. Metodología -----	9
4. Hallazgos por país y línea base regional-----	10
5. Hallazgos por país -----	11
5.1 Bahamas -----	11
5.2 Chile -----	11
5.3 Colombia -----	11
5.4 República Dominicana -----	11
5.5 Ecuador -----	11
5.6 Guatemala -----	12
5.7 México -----	12
5.8 Panamá-----	12
5.9 Uruguay -----	12
6. Brechas comunes, riesgos y áreas prioritarias de mejora-----	13
6.1 Brechas comunes observadas-----	13
6.2 Riesgos prioritarios -----	13
6.3 Áreas prioritarias de mejora -----	14
7. Análisis comparativo: línea base de LAC4 frente a referentes de la UE e internacionales -----	15
8. Panorama de Amenazas de ENISA — implicaciones para la región de ALC -----	17
9. Hoja de Ruta de Implementación -----	18
9.1 Fase 1 — Fundamentos (meses 1-6) -----	18
9.2 Fase 2 — Adopción en nuevas contrataciones (meses 6-12) -----	18
9.3 Fase 3 — Extensión a los contratos vigentes (meses 12-24) -----	18
9.4 Fase 4 — Mejora continua (año 2 en adelante)-----	19
9.5 Gobernanza y métricas para la evaluación continua -----	19
9.6 Necesidades de capacitación -----	19
10. Recomendaciones de seguridad -----	20
10.1 Planificación-----	20
10.2 Selección de proveedores y productos-----	28
10.3 Operaciones -----	40
10.4 Gestión de vulnerabilidades -----	48
10.5 Gestión de incidentes-----	54
10.6 Desmantelamiento / Fin de uso -----	58
11. Definiciones-----	63
12. Anexo A — Estándares para una Cadena de Suministro Cibersegura-----	65

A.1 Lista de Materiales de Software (SBOM)	65
A.2 Políticas de Divulgación de Vulnerabilidades (VDP)	65
A.3 Certificación de seguridad y niveles de aseguramiento	65
A.4 Ciclo de Vida de Desarrollo Seguro (SDL) e integridad del entorno de compilación	65
A.5 Gestión de vulnerabilidades — proveedor y entidad	66
A.6 Integridad del hardware (cuando se adquiere hardware)	66
A.7 Reporte de incidentes y penalidades contractuales	66
13. Anexo B — Guía práctica: evaluación mínima de riesgos de proveedores	67
B.1 Paso 1 — Caracterizar la contratación	67
B.2 Paso 2 — Identificar al proveedor y la profundidad de la cadena de suministro	67
B.3 Paso 3 — Identificar los escenarios de amenaza (utilizar la taxonomía de ENISA)	67
B.4 Paso 4 — Estimar la probabilidad y el impacto	67
B.5 Paso 5 — Identificar y escalonar los controles	67
B.6 Paso 6 — Decidir y documentar	67
B.7 Ejemplos de amenazas del Panorama de Amenazas de ENISA	68
B.8 Ejemplos de mitigaciones de estas directrices	68
14. Referencias	69

Prólogo

La transformación digital está redefiniendo la manera en que los gobiernos, los operadores de infraestructuras críticas y las instituciones públicas de América Latina y el Caribe prestan servicios, gestionan información y atienden a la ciudadanía. Al mismo tiempo, incrementa su dependencia de cadenas de suministro digitales complejas: proveedores de software, servicios en la nube, proveedores de servicios gestionados, fabricantes de hardware, integradores de sistemas y subcontratistas.

Esta interdependencia crea oportunidades, pero también riesgos compartidos. Una vulnerabilidad en un proveedor, una actualización de software comprometida, una supervisión insuficiente de subcontratistas o la ausencia de obligaciones contractuales claras en materia de seguridad pueden producir consecuencias que trascienden a una sola organización. Por ello, la contratación segura no debe entenderse únicamente como un proceso administrativo, sino como un componente esencial de la ciberresiliencia, la continuidad de los servicios y la confianza pública.

Estas *Prácticas Estandarizadas de Contratación Segura y Directrices de Ciberseguridad para la Cadena de Suministro* han sido desarrolladas para contribuir a afrontar este desafío. Ofrecen a las instituciones públicas, reguladores, operadores de infraestructuras críticas y demás organizaciones un marco práctico y adaptable para integrar la ciberseguridad a lo largo de todo el ciclo de vida de la contratación: desde la planificación y selección de proveedores, hasta las operaciones, la gestión de vulnerabilidades, la respuesta a incidentes y la terminación de la relación contractual.

Su relevancia para América Latina y el Caribe es especialmente significativa. La evaluación de línea base que sustenta este estudio muestra que, si bien la región ha alcanzado avances importantes en estrategias nacionales de ciberseguridad, mecanismos de gobernanza y capacidades de respuesta, los requisitos de ciberseguridad todavía no se incorporan de forma consistente en los procesos de contratación. Persisten brechas comunes en ámbitos como la evaluación de riesgos de los proveedores, las cláusulas contractuales modelo, la transparencia del software, la notificación de incidentes, la supervisión de subcontratistas, la portabilidad de datos y los planes de salida.

Las Directrices responden a estas brechas mediante un enfoque proporcional y basado en el riesgo. Sus recomendaciones están diseñadas para aplicarse según la criticidad de cada contratación, permitiendo a las instituciones establecer una línea base significativa y, a la vez, reservar controles más rigurosos para los servicios, sistemas y proveedores de mayor impacto. Este enfoque favorece una adopción práctica y reconoce los distintos niveles de madurez y capacidad institucional presentes en nuestra región.

Para LAC4, esta herramienta también representa un avance relevante en el fortalecimiento de la cooperación y la armonización entre la Unión Europea y América Latina y el Caribe. Las Directrices se nutren de marcos europeos de referencia, incluidos NIS2, el Reglamento de Ciberresiliencia, DORA, la Ley de Ciberseguridad de

la Unión Europea y las buenas prácticas de ENISA, y los articulan con normas y herramientas internacionalmente reconocidas, como las de ISO, NIST y CISA.

No se trata de reproducir mecánicamente normas europeas en un contexto distinto. Se trata de traducir buenas prácticas probadas en una referencia regional que pueda adaptarse a los marcos jurídicos, las prioridades institucionales y las realidades operativas de cada país. Al crear un lenguaje común sobre contratación segura y ciberseguridad de la cadena de suministro, estas Directrices pueden ayudar a reducir la fragmentación, promover la interoperabilidad y permitir que las instituciones públicas y los proveedores avancen hacia expectativas de seguridad más claras, coherentes y verificables.

LAC4 expresa su sincero agradecimiento a Florian Göhler y Predrag Tasevski, expertos técnicos y consultores cuyo conocimiento, análisis riguroso y compromiso hicieron posible este estudio. Agradecemos igualmente a los miembros de la comunidad LAC4 y a las instituciones que aportaron sus perspectivas, experiencia y participación continua durante este proceso. Su colaboración ha sido esencial para garantizar que las Directrices respondan a las necesidades de la región y, al mismo tiempo, se encuentren alineadas con las buenas prácticas europeas e internacionales.

Esperamos que esta publicación sea más que un documento de referencia. Debe constituir un punto de partida práctico para que las autoridades nacionales, los organismos de contratación, los equipos de ciberseguridad, los asesores jurídicos y los responsables de toma de decisiones fortalezcan la seguridad de los servicios digitales de los que nuestras sociedades dependen cada vez más.

La ciberseguridad de la cadena de suministro es un desafío transfronterizo. Abordarlo exige responsabilidad compartida, cooperación sostenida y un compromiso con la construcción de confianza en todo nuestro ecosistema digital. LAC4 se enorgullece de apoyar este esfuerzo colectivo y espera continuar trabajando con nuestros miembros y socios de toda la región para convertir estas Directrices en mejoras duraderas de la ciberresiliencia.

César Moliné Rodríguez

Director Regional

Centro de Cibercapacidades de Latinoamérica y el Caribe (LAC4)

1. Resumen Ejecutivo

Las entidades gubernamentales y los operadores de infraestructura crítica de la región de América Latina y el Caribe (ALC) dependen de cadenas de suministro digitales cada vez más complejas: software, hardware, servicios en la nube, servicios gestionados y una larga cadena de subencargados. El mismo ecosistema que hace posible la eficiencia también permite que la seguridad se vea comprometida. El informe de ENISA Threat Landscape for Supply Chain Attacks (2021) registró que los incidentes de cadena de suministro se cuadruplicaron entre 2020 y 2021, con un 66 % de los ataques dirigidos al código o a los procesos de los proveedores y un 62 % aprovechando la relación de confianza entre proveedor y cliente.

Este documento ofrece directrices estandarizadas, accionables y adaptables al contexto local, que integran la ciberseguridad en todo el ciclo de vida de la contratación y fortalecen la gestión de riesgos de la cadena de suministro en los organismos públicos y los sectores críticos. Incluye además la evaluación regional de línea base que motivó las decisiones de diseño adoptadas en las Directrices.

En los nueve Estados miembros de LAC4 para los que se dispuso de suficiente información pública, el patrón dominante es consistente: la ciberseguridad rara vez está integrada en los procesos de contratación, y el riesgo de la cadena de suministro no se aborda de manera estructurada. Dos países — Bahamas y Uruguay — tienen una cobertura parcial limitada a ámbitos específicos (infraestructura crítica o acceso de los proveedores a la información). Los demás países, o bien hacen referencia implícita a la cadena de suministro mediante un lenguaje general de gestión de riesgos, o bien no la abordan en absoluto.

Las Directrices están alineadas con la Directiva NIS2 de la UE, el Reglamento de Ciberresiliencia (CRA) de la UE, las Buenas Prácticas de ENISA para la Ciberseguridad de la Cadena de Suministro (junio de 2023), el Panorama de Amenazas de ENISA sobre Ataques a la Cadena de Suministro (julio de 2021), la Caja de Herramientas de la UE para la Cadena de Suministro de TIC, los esquemas de certificación de ciberseguridad de la UE EUCC y EUCS, y las normas técnicas de DORA. Incorporan las categorías de preguntas de la Plantilla SCRM para Proveedores del Grupo de Trabajo CISA / ICT SCRM y hacen referencia a las normas internacionales ISO/IEC 27036, ISO/IEC 27001:2022 y NIST SP 800-161 Rev. 1.

Estructura de las recomendaciones

El Capítulo 10 — Recomendaciones de seguridad contiene las 63 recomendaciones estandarizadas distribuidas en seis secciones, que reflejan el ciclo de vida de la contratación:

- 10.1 — Planificación (10 recomendaciones): gobernanza, alcance, restricciones, roles, participación de las partes interesadas, plan de integración, evaluación de riesgos, política, registro.
- 10.2 — Selección de proveedores y productos (18): jurisdicción, auditoría, ubicación, SGSI, SDL, integridad de la compilación, SBOM, vulnerabilidades, actualizaciones, VDP, portabilidad, certificaciones, riesgo del proveedor,

seguridad del personal, subencargados, cambio de control, requisitos de licitación, OEM / antifalsificación.

- 10.3 — Operaciones (12): reevaluación anual, intercambio de información sobre amenazas, capacitación, endurecimiento (hardening), respaldos, RACI, contratos, identidad y acceso, segmentación, aplicación de parches, código de conducta.
- 10.4 — Gestión de vulnerabilidades (8): PSIRT, análisis de vulnerabilidades y debilidades, análisis de causa raíz, política de mantenimiento basada en CVSS, notificación a clientes, gestión de vulnerabilidades del lado de la entidad con monitoreo de SBOM, prueba de parches y reversión, divulgación coordinada de vulnerabilidades.
- 10.5 — Gestión de incidentes (8): canales de comunicación, RTO, BCP, pruebas de restauración, guías de respuesta conjuntas, notificación contractual, penalidades, revisión posterior al incidente.
- 10.6 — Desmantelamiento / Fin de uso (7): plan, partes interesadas, exportación de datos, eliminación, desactivación, continuidad del acuerdo de confidencialidad, sanitización del hardware.

Hallazgos clave de la línea base regional

- La mayoría de los Estados miembros de LAC4 analizados no cuenta con un marco estandarizado de contratación segura que aborde específicamente la ciberseguridad.
- Donde existen disposiciones sobre la cadena de suministro (Bahamas, Uruguay), estas son parciales — limitadas a la infraestructura crítica o a aspectos específicos (acceso de los proveedores a la información).
- Existe una amplia alineación con las normas internacionales en abstracto, pero una orientación operativa limitada, y pocas cláusulas modelo o herramientas de evaluación de riesgos de proveedores a nivel nacional.
- Todos los países estudiados se beneficiarían de cláusulas modelo estandarizadas, un cuestionario para proveedores, un requisito de SBOM, integridad del entorno de compilación (build pipeline), un régimen específico de gestión de vulnerabilidades y una obligación de plan de salida.

Entregables complementarios

- Cláusulas Modelo y Mapeo (Excel) — cuestionario para proveedores de 63 preguntas, tabla de correspondencia entre múltiples marcos y cláusulas contractuales listas para copiar y pegar.
- Presentación de Difusión — diapositivas para la adopción nacional y los talleres con las partes interesadas.

2. Introducción

2.1 Contexto y objetivos

La región de ALC ha acelerado su transformación digital en la última década. Los servicios públicos, los servicios financieros, los servicios de salud y los operadores de energía dependen de cadenas de suministro digitales largas y opacas. Los informes regionales recientes — incluido el Reporte de Ciberseguridad 2025 del BID / OEA — identifican de manera consistente la seguridad de la cadena de suministro y la seguridad de las contrataciones como áreas de baja madurez en toda la región.

EU CyberNet, a través de la Convocatoria de Acción CFA-215, solicitó el desarrollo de directrices integrales sobre contratación segura y gestión ciberresiliente de la cadena de suministro para apoyar a la comunidad de práctica LAC4. Este documento es el entregable principal que responde a esa solicitud.

2.2 Alcance y destinatarios

Estas directrices están dirigidas a las entidades — organismos públicos, reguladores, operadores de infraestructura crítica y cualquier organización que adquiera servicios y productos digitales. Se centran principalmente en las entidades esenciales e importantes en el sentido de la Directiva NIS2 de la UE, pero están redactadas para ser adaptables a organizaciones de cualquier tamaño.

Cubren las cadenas de suministro digitales en sentido amplio: software, hardware, servicios en la nube, servicios gestionados y cualquier tercero que procese información de la entidad u opere un sistema en su nombre — fabricantes, distribuidores, integradores de sistemas, MSP, MSSP y proveedores de servicios digitales, según la tipología utilizada en las Buenas Prácticas de ENISA de 2023.

2.3 Cómo utilizar este documento

El Capítulo 10 es una lista de verificación de 63 recomendaciones. Cada recomendación está formulada como una pregunta que la entidad debería poder responder. Debajo de la pregunta, una línea de Criticidad indica el nivel de criticidad de la contratación a partir del cual la recomendación pasa a ser obligatoria:

- Baja — obligatoria en todos los niveles (contrataciones de criticidad Baja, Media y Alta).
- Media — obligatoria en las contrataciones de criticidad Media y Alta.
- Alta — obligatoria solo en las contrataciones de criticidad Alta (los controles más exigentes).

Cada recomendación incluye una Justificación, Ejemplos prácticos e información adicional, y un Mapeo a las normas y marcos pertinentes. Cuando corresponde, se presenta un caso ilustrativo del Panorama de Amenazas de ENISA.

Las entidades pueden utilizar el Excel de Mapeo complementario (entregable 4 de la Convocatoria de Acción) como cuestionario para proveedores — que incluye el mismo filtro de niveles que señala qué preguntas son obligatorias según la criticidad Baja, Media o Alta — y como tabla de correspondencia entre múltiples marcos.

3. Metodología

La metodología detrás de este borrador consolidado siguió cinco pasos, fusionando el trabajo que produjo las Directrices y el trabajo que produjo el Informe de Evaluación de Línea Base.

- (i) Revisión documental de las estrategias nacionales de ciberseguridad, las leyes marco y las políticas de contratación de los Estados miembros de LAC4 para los que había información pública disponible, además de los estudios regionales (en particular, el Reporte de Ciberseguridad 2025 del BID / OEA sobre los desafíos de vulnerabilidad y madurez para cerrar las brechas en América Latina y el Caribe).
- (ii) Análisis comparativo frente a las normas de la UE (NIS2, CRA, Ley de Ciberseguridad de la UE, Buenas Prácticas de ENISA para la Ciberseguridad de la Cadena de Suministro (junio de 2023), Panorama de Amenazas de ENISA sobre Ataques a la Cadena de Suministro (julio de 2021), Guía de Implementación Técnica de ENISA para el Reg. (UE) 2024/2690, RTS de DORA 1773, 1774 y 532) y referencias internacionales complementarias (ISO/IEC 27036, ISO/IEC 27001:2022, NIST SP 800-161 Rev.1, NIST SSDF, Plantilla SCRM para Proveedores de CISA).
- (iii) Análisis de contenido para extraer las familias de controles recurrentes y las cinco áreas de enfoque de las Buenas Prácticas de ENISA (Enfoque corporativo estratégico, Gestión de riesgos de la cadena de suministro, Gestión de las relaciones con los proveedores, Gestión de vulnerabilidades, Calidad de los productos y las prácticas).
- (iv) Mapeo de las ocho categorías de preguntas de la Plantilla SCRM de CISA — Calificación, SCM y Gobernanza, Diseño Seguro, Seguridad de la Información, Seguridad Física, Personal, Integridad de la Cadena de Suministro, Resiliencia — a la estructura de capítulos de las Directrices, para garantizar que ninguna categoría de la Plantilla SCRM quede sin cubrir.
- (v) Consolidación en un formato de directrices basado en preguntas y anclado en mapeos, con un nivel de criticidad por pregunta (Baja / Media / Alta) que el Excel de Mapeo complementario utiliza como cuestionario para proveedores.

Limitaciones de cobertura: esta evaluación se basa en información disponible públicamente. Tres países de LAC4 — Antigua y Barbuda, El Salvador y Costa Rica — no pudieron ser analizados dentro del plazo del proyecto y quedan señalados para la fase 2 (wave-2) de la etapa de validación.

4. Hallazgos por país y línea base regional

Las recomendaciones de este documento están calibradas según la madurez actual de los Estados miembros de LAC4. Esta sección resume la evaluación de línea base realizada en nueve de los doce Estados miembros de LAC4.

País	Región	Cobertura	Hallazgos
Bahamas	Caribe	Parcial — solo IC	El Objetivo 8 de la estrategia nacional aborda la cadena de suministro y las relaciones con terceros, con alcance limitado al gobierno y la IC. No existe un marco estandarizado de contratación ni directrices de aplicación general para la cadena de suministro.
Chile	Sur	No definida	La Política Nacional de Ciberseguridad 2023-2028 y la Ley Marco de Ciberseguridad (ANCI) no cubren explícitamente la contratación segura. Según el NCSI, no se ha establecido formalmente un marco nacional estandarizado.
Colombia	Andina	No abordada	La estrategia nacional y la reciente agenda digital no abordan la ciberseguridad en la contratación, las adquisiciones ni la cadena de suministro.
República Dominicana	Caribe	Indirecta / parcial	La estrategia mejora el marco regulatorio y la gobernanza de las TIC, lo que puede impulsar implícitamente estándares mínimos de seguridad. No existe un marco estandarizado detallado (sin SBOM, certificación ni verificación de proveedores). La cadena de suministro se limita a referencias a la IC.
Ecuador	Andina	No abordada	La seguridad de las contrataciones no es un componente diferenciado de la estrategia. La cadena de suministro aparece de forma implícita en el lenguaje de gestión de riesgos, pero no está formalizada.
Guatemala	Central	No abordada	La estrategia nacional no contiene disposiciones operativas. No hay evidencia de estándares de ciberseguridad utilizados en los procesos de contratación.
México	Central	No abordada	La Estrategia Nacional de Ciberseguridad no menciona la cadena de suministro ni la contratación. La regulación de ciberseguridad está fragmentada por sectores y se centra mayormente en la protección de datos.
Panamá	Central	No abordada (tratado)	No se documenta un régimen nacional pertinente para la cadena de suministro (NCSI). Un acuerdo bilateral con el SOUTHCOM de EE. UU. cubre aspectos de la cadena de suministro, pero la información pública es limitada.
Uruguay	Sur	La más desarrollada (aún parcial)	El marco de AGESIC incluye una Política de Relacionamiento con Proveedores (concisa, centrada en el acceso de los proveedores a la información) y requisitos de seguridad para proveedores de software (mayormente técnicos). Los planes de salida, el SBOM, el riesgo de cuartas partes y la respuesta conjunta a incidentes permanecen mayormente sin abordar.

5. Hallazgos por país

5.1 Bahamas

La Estrategia Nacional de Ciberseguridad contiene un Objetivo 8 que aborda la cadena de suministro y las relaciones con terceros, pero solo en el ámbito del gobierno y la infraestructura crítica. La estrategia no incluye prácticas estandarizadas de contratación segura ni directrices integrales de ciberseguridad para la cadena de suministro aplicables a todos los sectores. En consecuencia, no existen cláusulas modelo, ni requisito de SBOM, ni obligación de plan de salida. Para efectos de estas Directrices, Bahamas se ubica en la mitad superior de la línea base regional por el reconocimiento explícito del tema, pero carece de herramientas operativas.

5.2 Chile

La Política Nacional de Ciberseguridad 2023-2028 de Chile y la Ley Marco de Ciberseguridad (que otorga facultades a la ANCI) definen la gobernanza general de la ciberseguridad, pero no cubren explícitamente la contratación segura. Según el NCSI, aún no se ha establecido formalmente un marco nacional estandarizado sobre contratación segura. La combinación de un regulador emergente (ANCI) y una actualización de la política nacional crea una ventana de oportunidad para incorporar estas Directrices en la regulación subordinada.

5.3 Colombia

La estrategia nacional de ciberseguridad de Colombia y la agenda digital / de IA recientemente emitida por el MinTIC no abordan de manera estructurada la ciberseguridad en la contratación, las adquisiciones ni la cadena de suministro. La contratación del sector público se rige por la Ley 80/1993 y sus normas sucesoras, y la ciberseguridad se aborda solo de forma indirecta mediante requisitos generales de protección de datos. La ausencia de una dimensión estructurada de cadena de suministro es la brecha principal.

5.4 República Dominicana

La cobertura es parcial e indirecta. La estrategia fortalece el marco legal y regulatorio de la ciberseguridad y mejora la gobernanza de los sistemas TIC del gobierno, lo que puede impulsar implícitamente estándares mínimos de seguridad en la contratación. Sin embargo, la estrategia no contiene un marco estandarizado y detallado de contratación segura comparable al modelo de la UE — no hay requisito de SBOM, certificación de proveedores ni verificación formal. Las directrices de cadena de suministro se limitan a referencias en la protección de infraestructura crítica y la respuesta a incidentes, y no a los procesos generales de contratación.

5.5 Ecuador

La seguridad de las contrataciones no es un componente diferenciado de la estrategia nacional de ciberseguridad. Los temas de cadena de suministro aparecen de forma implícita en el lenguaje general de gestión de riesgos, pero no están formalizados. No existe un cuestionario nacional para proveedores publicado ni un catálogo nacional

de cláusulas modelo de seguridad. La oportunidad aquí consiste en anclar las Directrices en la ley nacional de contratación pública mediante una circular emitida por la autoridad central de contrataciones.

5.6 Guatemala

No hay evidencia del uso de estándares de ciberseguridad como guía de los procesos de contratación. La estrategia nacional no contiene disposiciones operativas sobre contratación segura ni sobre ciberseguridad de la cadena de suministro. Las Directrices pueden adoptarse como documento fundacional sobre el cual construir un enfoque nacional.

5.7 México

La Estrategia Nacional de Ciberseguridad no menciona la cadena de suministro ni la contratación. La regulación de ciberseguridad en México está fragmentada por sectores (el regulador financiero CNBV, el regulador de telecomunicaciones IFT, el INAI para la protección de datos) y se centra mayormente en la protección de datos más que en la ciberseguridad, sin un régimen uniforme. Una aplicación transversal y por niveles de las Directrices es la vía más realista.

5.8 Panamá

No se documenta en el NCSI un régimen nacional pertinente de seguridad de la cadena de suministro. Un acuerdo de cooperación bilateral con el Comando Sur de los Estados Unidos cubre aspectos de la cadena de suministro, pero la información pública es limitada. El CSIRT adscrito a la Autoridad Nacional para la Innovación Gubernamental (AIG) es la contraparte operativa más probable para la adopción de estas Directrices.

5.9 Uruguay

Uruguay tiene el marco nacional más desarrollado del grupo analizado. El marco nacional de ciberseguridad administrado por AGESIC incluye una Política de Relacionamiento con Proveedores (concisa — alrededor de una página de contenido — centrada principalmente en el acceso de los proveedores a la información más que en la seguridad de los servicios o productos adquiridos) y un conjunto de requisitos de seguridad para proveedores de software (mayormente técnicos, con algunos requisitos organizacionales). Otros temas de la cadena de suministro — planes de salida, SBOM, riesgo de cuartas partes y respuesta conjunta a incidentes — permanecen mayormente sin abordar. Uruguay es, por lo tanto, el adoptante piloto natural de las Directrices completas, sobre la base de los instrumentos existentes.

6. Brechas comunes, riesgos y áreas prioritarias de mejora

6.1 Brechas comunes observadas

- No existe un marco estandarizado de seguridad de las contrataciones aplicable a todos los sectores — donde existe cobertura, es parcial (solo IC) o de un solo aspecto.
- No hay cláusulas modelo de seguridad ni plantillas de licitación disponibles a nivel nacional para que las entidades contratantes las reutilicen.
- No se exige una Lista de Materiales de Software (SBOM) en las licitaciones ni en los contratos.
- Las obligaciones de divulgación de vulnerabilidades de los proveedores no están estandarizadas y rara vez se incorporan en los contratos.
- Las expectativas de integridad del código y del entorno de compilación (build pipeline) para los proveedores de software no están articuladas, a pesar de los conocidos incidentes de SolarWinds y Codecov.
- Las metodologías de evaluación de riesgos de proveedores no están armonizadas; las entidades reinventan los cuestionarios en cada licitación, con una variación significativa en la cobertura.
- Las obligaciones de salida y desmantelamiento están mayormente ausentes, lo que expone a las entidades a la dependencia del proveedor (vendor lock-in) y a riesgos de continuidad.
- El riesgo de cuartas partes (subencargados, cadena de suministro del proveedor) rara vez se aborda en el marco de algún país.
- Los plazos de notificación de incidentes y las penalidades contractuales no están estandarizados en los contratos de adquisición.
- Las obligaciones de seguridad del personal del proveedor no se hacen cumplir de manera consistente mediante cláusulas contractuales.
- La gestión de vulnerabilidades — del lado del proveedor (PSIRT, análisis formal de vulnerabilidades y debilidades, retroalimentación de causa raíz hacia el SDL) y del lado de la entidad (programa interno de gestión de vulnerabilidades, monitoreo de SBOM, prueba de parches y reversión, participación en CVD) — se trata como un único renglón, cuando las Buenas Prácticas de ENISA la identifican como un área de enfoque diferenciada.

6.2 Riesgos prioritarios

A partir de las brechas anteriores, los riesgos más relevantes para las entidades de la región son:

- Ataques a la cadena de suministro mediante actualizaciones de software comprometidas o dependencias de código abierto comprometidas (mitigados por SBOM, SDL, integridad del entorno de compilación, VDP, PSIRT).

- Riesgo de dependencia (lock-in) y de continuidad — incapacidad de migrar cargas de trabajo críticas, especialmente cuando los proveedores operan desde fuera de la región (mitigado por la portabilidad de los datos y los planes de salida).
- Riesgo no gestionado de subencargados — la entidad no puede enumerar ni controlar su exposición a cuartas partes (mitigado por cláusulas de aprobación y notificación de subencargados).
- Notificación lenta de incidentes — la entidad no puede cumplir sus propias obligaciones equivalentes a NIS2 porque el proveedor no notificó a tiempo (mitigado por plazos contractuales de notificación).
- Compromiso del acceso privilegiado del personal del proveedor (mitigado por la verificación del personal, cuentas nominativas, MFA, elevación JIT y segmentación).
- Integridad del hardware (componentes falsificados / no OEM) en las adquisiciones de los sectores de transporte, energía y defensa (mitigada por el abastecimiento exclusivo de OEM y embalajes que evidencien cualquier apertura o manipulación).

6.3 Áreas prioritarias de mejora

- Adoptar estas Directrices como referencia nacional — publicada por la autoridad nacional de ciberseguridad — para el sector público y los sectores críticos.
- Emitir cláusulas modelo estandarizadas (seguridad, auditoría, notificación de incidentes, portabilidad de datos, aprobación de subencargados, salida, continuidad del acuerdo de confidencialidad, integridad de la compilación, abastecimiento exclusivo de OEM).
- Hacer obligatorio el cuestionario para proveedores del Excel de Mapeo como parte de la precalificación de cualquier contratación por encima de un umbral nacional.
- Exigir un SBOM, una Política de Divulgación de Vulnerabilidades publicada y una función equivalente a un PSIRT a los proveedores de software / servicios digitales.
- Adoptar un enfoque por niveles de riesgo: controles más fuertes para los proveedores de servicios críticos / esenciales y controles más ligeros para las contrataciones de bajo riesgo — la etiqueta de nivel de cada recomendación de este documento ya implementa este enfoque.
- Habilitar el intercambio regional de información sobre proveedores con problemas reiterados de ciberseguridad (comunidad de práctica LAC4).

7. Análisis comparativo: línea base de LAC4 frente a referentes de la UE e internacionales

La siguiente tabla mapea cada área de control de las Directrices con el referente pertinente de la UE / internacional, la línea base esperada y el estado agregado en los Estados miembros de LAC4. La columna de áreas de control está anclada en las cinco áreas de enfoque de las Buenas Prácticas de ENISA para la Ciberseguridad de la Cadena de Suministro (2023) — enfoque corporativo estratégico, gestión de riesgos de la cadena de suministro, gestión de las relaciones con los proveedores, gestión de vulnerabilidades y calidad de los productos y las prácticas — para facilitar la alineación con la política de la UE.

Área de control / enfoque de las BP de ENISA	Referente UE / internacional	Línea base esperada	Estado LAC4 (agregado)
Enfoque corporativo estratégico (BP ENISA 3.1)	NIS2 Art. 21(2)(d), ISO 27036-2 cl. 6, CISA SCRM P. 2.3	Establecer política, alcance, lista de proveedores vetados, rol designado, RACI	Mayormente ausente; Uruguay parcial. Estudio de ENISA 2023: el 76 % de las organizaciones de la UE también carece de roles dedicados a la cadena de suministro.
Gestión de riesgos de la cadena de suministro (BP ENISA 3.2)	ISO 27005, ENISA TIG 2024/2690	Registro de riesgos por proveedor con nivel de criticidad y frecuencia de revisión	No estandarizada en ninguna estrategia de LAC4. Estudio de ENISA 2023: solo el 37 % de las organizaciones de la UE realiza evaluaciones de riesgo de sus proveedores.
Gestión de las relaciones con los proveedores — Auditoría (BP 3.3)	RTS de DORA 1773; ISO 27036-2; CISA SCRM P. 4.17, 7.9	Derecho de auditoría; ISO 27001 / SOC 2 / EUCC / EUCS cuando corresponda	Las cláusulas de auditoría aparecen de forma ad hoc; el aseguramiento basado en certificaciones no está incorporado en las licitaciones.
Gestión de vulnerabilidades (BP 3.4) — SBOM	CRA de la UE, Anexo I, Parte II; SBOM de CISA / NTIA; CISA SCRM P. 2.5	SBOM legible por máquina (CycloneDX / SPDX) en la entrega y en cada versión mayor	Ningún país lo exige.
Gestión de vulnerabilidades (BP 3.4) — VDP	CRA de la UE, Arts. 13-14; ISO 29147 / 30111	VDP pública; obligaciones de actualizaciones de seguridad con aviso previo	No estandarizada a nivel regional.
Gestión de vulnerabilidades (BP 3.4) — Programa y PSIRT	BP ENISA 3.4; CISA SCRM §3.14-3.17, §4.14-4.23; marco PSIRT de FIRST.org	PSIRT del lado del proveedor, análisis formal de vulnerabilidades/debilidades, retroalimentación de causa raíz, política de	Ningún país de LAC4 exige un PSIRT del proveedor ni un programa de gestión de vulnerabilidades del lado de la entidad

Área de control / enfoque de las BP de ENISA	Referente UE / internacional	Línea base esperada	Estado LAC4 (agregado)
		mantenimiento basada en CVSS, notificación proactiva a los clientes — junto con un programa interno de gestión de vulnerabilidades del lado de la entidad, monitoreo de SBOM, prueba de parches y reversión, y participación en CVD	basado en SBOM. Los regímenes de CVD están mayormente ausentes.
Calidad de los productos (BP ENISA 3.5) — Desarrollo seguro	NIS2 Art. 21(3); NIST SSDF; CISA SCRM P. 3.10	SDL documentado con revisión por pares, modelado de amenazas y pruebas de seguridad	Ausente de los marcos de contratación.
Calidad de los productos (BP 3.5) — Integridad del entorno de compilación	CISA SCRM P. 3.6, 3.7, 3.13; SLSA de Google	Firma de código, compilaciones reproducibles, entornos de compilación controlados	No abordada — aun cuando SolarWinds y Codecov son casos bien conocidos.
Subencargados / cuartas partes	RTS de DORA 532; NIS2 Art. 22; CISA SCRM P. 2.10	Lista, aprobación previa, cláusulas de aplicación en cascada (flow-down), derechos de auditoría	No abordado.
Seguridad del personal	ISO 27001 Anexo A.6; CISA SCRM P. 6.1-6.6	Procesos de verificación, incorporación y desvinculación trasladados contractualmente	No estandarizada mediante cláusulas de contratación.
Notificación de incidentes (BP 3.3)	NIS2 Art. 23; CISA SCRM P. 4.25	Plazo contractual alineado con las propias obligaciones NIS2 de la entidad	Los regímenes nacionales varían; no se trasladan a los contratos con proveedores.
Portabilidad de datos / salida	Ley de Datos de la UE; ENISA Cloud RA	Formato de exportación no propietario, plan de salida validado	Mayormente ausente (Uruguay parcial).
Continuidad y pruebas de salida	DORA Art. 28; ISO 22301; CISA SCRM P. 8.3	Plan de salida probado al menos cada 24 meses; se considera la diversidad de proveedores	No estandarizado.

8. Panorama de Amenazas de ENISA — implicaciones para la región de ALC

El Panorama de Amenazas de ENISA sobre Ataques a la Cadena de Suministro (julio de 2021) catalogó 24 incidentes de cadena de suministro reportados entre enero de 2020 e inicios de julio de 2021. Los hallazgos principales, y la forma en que dan forma a estas Directrices, se resumen a continuación.

- El 66 % de los ataques se dirigió al código o a los procesos de los proveedores (p. ej., SolarWinds Orion, Codecov) — incorporado en S-08 (SDL) y S-18 (integridad del entorno de compilación).
- El 62 % de las vulneraciones de clientes aprovechó la relación de confianza con el proveedor (canales de actualización automática, certificados firmados, etc.) — abordado por S-06 (SBOM), S-09 (VDP y actualizaciones de seguridad), I-05 (guías de respuesta conjuntas), O-10 (segmentación) y todo el Capítulo 4 (Gestión de vulnerabilidades).
- El 66 % de los proveedores no sabía cómo fue comprometido o no fue transparente al respecto — lo que motiva directamente O-02 (intercambio de información), V-05 (notificación a clientes), V-08 (CVD), I-06 (notificación) e I-08 (revisión posterior al incidente).
- Más del 50 % de los incidentes se atribuyó a grupos APT — lo que sustenta que incluso los ecosistemas de proveedores maduros requieren defensa en profundidad (O-09 cuentas nominativas / MFA / JIT, O-10 segmentación, O-06 respaldos independientes).
- ENISA recomienda que los clientes identifiquen y documenten los tipos de proveedores, definan criterios de riesgo, gestionen a los proveedores a lo largo del ciclo de vida y definan obligaciones de protección, intercambio de información, auditoría, continuidad del negocio, verificación del personal y gestión de incidentes — cada una de estas recomendaciones está operacionalizada en las Directrices.

9. Hoja de Ruta de Implementación

Estas directrices están diseñadas para adoptarse de manera progresiva. Una implementación por fases reduce el riesgo de interrupción de las contrataciones en curso y permite el desarrollo de capacidades.

9.1 Fase 1 — Fundamentos (meses 1-6)

- El coordinador nacional (autoridad de ciberseguridad o CSIRT) respalda las directrices y las publica como orientación oficial.
- Cada entidad adoptante designa un Oficial de Ciberseguridad con mandato sobre la cadena de suministro e identifica un punto focal de seguridad de las contrataciones.
- Cada entidad adoptante establece una política de seguridad de la cadena de suministro y un grupo de gobernanza de contrataciones (legal, TI/seguridad, compras, dueños de negocio).
- Cada entidad adoptante construye un inventario de los proveedores críticos existentes y los clasifica por criticidad (utilizando el mismo esquema Baja / Media / Alta de este documento).

9.2 Fase 2 — Adopción en nuevas contrataciones (meses 6-12)

- Aplicar las secciones 10.1 (Planificación) y 10.2 (Selección) a todas las nuevas licitaciones.
- Incorporar las cláusulas modelo (derechos de auditoría, notificación de incidentes, portabilidad de datos, salida, continuidad del acuerdo de confidencialidad, aprobación de subencargados, integridad de la compilación, exclusividad OEM) en las plantillas contractuales estándar.
- Hacer obligatorio el cuestionario para proveedores (Excel de Mapeo) para cualquier contratación por encima de un umbral nacional o relacionada con una entidad crítica o esencial.
- Hacer obligatorios el SBOM, la VDP y un PSIRT del proveedor para cualquier contratación de software / servicios digitales.

9.3 Fase 3 — Extensión a los contratos vigentes (meses 12-24)

- Aplicar la sección 10.3 (Operaciones) y la sección 10.4 (Gestión de vulnerabilidades) a las relaciones existentes con proveedores mediante enmiendas contractuales al momento de la renovación.
- Implementar la reevaluación anual del riesgo de los proveedores.
- Desarrollar guías de respuesta conjuntas a incidentes con los proveedores críticos.
- Validar los planes de salida / desmantelamiento con los proveedores más críticos.

9.4 Fase 4 — Mejora continua (año 2 en adelante)

- La autoridad nacional publica una evaluación anual de madurez.
- Se agregan especializaciones sectoriales (anexo del sector financiero alineado con DORA, anexo de salud).
- Se establece a través de LAC4 el intercambio de inteligencia sobre proveedores (desidentificada) entre países de ALC.
- La integración con las estrategias nacionales existentes y las iniciativas de transformación digital se revisa cada 12 meses.

9.5 Gobernanza y métricas para la evaluación continua

Las autoridades adoptantes deberían dar seguimiento, como mínimo, a las siguientes métricas:

- Porcentaje de nuevas licitaciones que incluyen las cláusulas estándar de seguridad.
- Porcentaje de proveedores que han completado el cuestionario para proveedores.
- Porcentaje de contrataciones de software / servicios digitales que incluyen un SBOM.
- Número de incidentes de cadena de suministro notificados por los proveedores dentro de los plazos contractuales.
- Tiempo promedio para revocar el acceso del proveedor al finalizar el contrato.
- Número de proveedores críticos con un plan de salida probado.

9.6 Necesidades de capacitación

- Oficiales de compras: fundamentos de contratación segura, cláusulas modelo, interpretación del cuestionario para proveedores.
- Oficiales de ciberseguridad / CISO: metodología de evaluación de riesgos de proveedores, análisis de SBOM, gestión de vulnerabilidades (PSIRT, CVD, análisis de causa raíz), gestión de incidentes con proveedores, evaluación de la integridad del entorno de compilación.
- Asesores legales: mecanismos contractuales para auditorías transfronterizas, aprobación de subencargados, localización de datos, cooperación con los reguladores.
- Alta dirección: supervisión del riesgo de la cadena de suministro; definición del apetito de riesgo.

10. Recomendaciones de seguridad

Esta sección contiene las 63 recomendaciones estandarizadas distribuidas en seis secciones, que reflejan el ciclo de vida de la contratación. Cada recomendación está formulada como una pregunta que la entidad debería poder responder. La línea de Criticidad debajo de la pregunta indica el nivel de criticidad de la contratación a partir del cual la recomendación pasa a ser obligatoria: Baja (obligatoria en todos los casos), Media (obligatoria en Media y Alta) o Alta (obligatoria solo en Alta). Cada pregunta va seguida de una Justificación, Ejemplos prácticos e información adicional, un caso ilustrativo opcional del Panorama de Amenazas de ENISA y un Mapeo a las normas y marcos pertinentes.

Las secciones 10.1 a 10.6 a continuación corresponden a las seis secciones de las Directrices:

- 10.1 — Planificación (10 recomendaciones)
- 10.2 — Selección de proveedores y productos (18 recomendaciones)
- 10.3 — Operaciones (12 recomendaciones)
- 10.4 — Gestión de vulnerabilidades (8 recomendaciones)
- 10.5 — Gestión de incidentes (8 recomendaciones)
- 10.6 — Desmantelamiento / Fin de uso (7 recomendaciones)

10.1 Planificación

La planificación establece el alcance, la gobernanza y las restricciones bajo las cuales se llevará a cabo cualquier contratación. Las decisiones tomadas en la etapa de planificación determinan qué puede — y qué no puede — adquirirse, quién es responsable y qué requisitos mínimos aplican. El Artículo 21(2)(d) de NIS2 y las Buenas Prácticas de ENISA para la Ciberseguridad de la Cadena de Suministro (2023) exigen a las entidades definir la seguridad de la cadena de suministro como una actividad gestionada, no como una tarea puntual.

P-01 ¿Existe una estrategia aprobada por la dirección que determine qué servicios y productos pueden adquirirse de terceros?

Criticidad: Baja · Obligatoria en todos los niveles de criticidad (Baja, Media, Alta).

Justificación

Casi toda actividad digital puede contratarse con proveedores y suplidores. Sin embargo, en algunos casos una actividad es tan sensible que no debería realizarse en infraestructura de terceros — por ejemplo, cuando una entidad determina que ciertos datos de negocio son altamente confidenciales, o cuando las leyes de protección de datos o los contratos existentes prohíben determinadas acciones.

Sin una estrategia explícita, las decisiones individuales de contratación se toman de forma aislada y pueden terminar exponiendo datos o capacidades que la entidad pretendía mantener internamente. Las Buenas Prácticas de ENISA para la Ciberseguridad de la Cadena de Suministro identifican el enfoque corporativo

estratégico como la primera de cinco áreas de enfoque para las entidades esenciales e importantes.

Ejemplos e información adicional

La alta dirección debería adoptar una política vinculante que defina (i) qué categorías de datos y qué actividades de misión crítica no pueden tercerizarse, (ii) qué categorías pueden tercerizarse solo bajo condiciones restrictivas (p. ej., solo en el territorio nacional, solo con proveedores certificados), y (iii) qué categorías están abiertas a la contratación estándar.

La política debería revisarse al menos una vez al año y después de cualquier cambio importante en el entorno regulatorio.

- Categorías de datos que deben permanecer internas (p. ej., información clasificada, judicial, de inteligencia).
- Categorías de datos que pueden ser procesadas por terceros solo bajo condiciones específicas (p. ej., datos personales de los ciudadanos — en el territorio nacional, con proveedor certificado).
- Actividades que pueden tercerizarse libremente (p. ej., productividad de oficina genérica, sitios web de cara al público).

Mapeo

Marco	Referencia / cláusula
Directiva NIS2	Art. 21(2)(d) — la seguridad de la cadena de suministro como parte de las medidas de gestión de riesgos
Buenas Prácticas de ENISA para la Ciberseguridad de la Cadena de Suministro (2023)	Área 3.1 — Enfoque corporativo estratégico
ISO/IEC 27036-2	Cláusula 6 — Seguridad de la información en las relaciones con los proveedores
NIST SP 800-161 Rev. 1	Sección 2.3 — Estrategia C-SCRM
Plantilla SCRM de CISA	P. 2.3 — Estrategia integral a nivel de toda la organización

P-02 ¿Se consideran y documentan las restricciones externas e internas para la contratación (sanciones, proveedores vetados, país de origen, protección de datos, contratos contradictorios)?

Criticidad: Baja · Obligatoria en todos los niveles de criticidad (Baja, Media, Alta).

Justificación

Las entidades pueden necesitar evitar a ciertos terceros por razones legales o estratégicas: regímenes de sanciones, incidentes previos que involucren a un proveedor, normas de protección de datos que limiten las transferencias transfronterizas, contratos contradictorios con otras partes o restricciones de seguridad nacional sobre el origen de la tecnología.

Si los oficiales de compras no tienen acceso a una lista actualizada de restricciones, los problemas se descubren tarde — típicamente en la revisión del contrato — lo que genera esfuerzos desperdiciados y retrasos. La Plantilla SCRM para Proveedores de

CISA (P. 2.4 / 4.9) convierte la verificación de la lista de vetados en un control independiente.

Ejemplos e información adicional

La función de compras, en coordinación con los asesores legales y el oficial de ciberseguridad, debería mantener una lista de restricciones y circularla a todos los empleados pertinentes. La lista debería revisarse cada vez que se actualicen las sanciones internacionales y cada vez que una autoridad nacional emita una alerta sobre un proveedor.

- Proveedor con problemas de ciberseguridad conocidos y reiterados
- Sanciones y embargos
- Leyes de protección de datos que restringen las transferencias transfronterizas
- Contratos contradictorios existentes con otras partes
- Restricciones de seguridad nacional sobre el origen de la tecnología
- Políticas existentes de la entidad sobre proveedores vetados

Mapeo

Marco	Referencia / cláusula
Caja de Herramientas de la UE para la Cadena de Suministro de TIC	Escenarios de riesgo — dependencia estratégica de proveedores de alto riesgo
Directiva NIS2	Art. 22 — evaluaciones coordinadas de riesgos de seguridad de las cadenas de suministro críticas
Plantilla SCRM de CISA	P. 2.4 componentes vetados, P. 4.9 activos vetados
NIST SP 800-161 Rev. 1	Sección 3 — Propiedad, control o influencia extranjeros

P-03 ¿Ha designado la entidad un oficial de ciberseguridad con un mandato explícito sobre la cadena de suministro?

Criticidad: Baja · Obligatoria en todos los niveles de criticidad (Baja, Media, Alta).

Justificación

La ciberseguridad es una actividad cotidiana del personal de TI, pero la gestión estratégica de la ciberseguridad — incluidos los aspectos de la cadena de suministro — debe asignarse a un rol dedicado.

El estudio de ENISA de 2023 encontró que el 76 % de las organizaciones encuestadas no tenía roles ni responsabilidades dedicados a la ciberseguridad de la cadena de suministro de TIC/OT. Sin un rol de este tipo, el riesgo de la cadena de suministro queda entre la función de compras (enfocada en el costo y el cronograma) y la de TI (enfocada en la estabilidad operativa), y rara vez se aborda de manera proactiva.

Ejemplos e información adicional

El oficial de ciberseguridad (CISO o equivalente) debería contar con un mandato escrito que incluya explícitamente la ciberseguridad de la cadena de suministro. El rol debería situarse a un nivel suficientemente alto como para cuestionar decisiones de contratación y reportar a la alta dirección.

Mapeo

Marco	Referencia / cláusula
Buenas Prácticas de ENISA (2023)	Área 3.1 — rol designado para el riesgo de proveedores
ISO/IEC 27001:2022	Cláusula 5.3 — Roles, responsabilidades y autoridades organizacionales
Directiva NIS2	Art. 20 — responsabilidad de los órganos de dirección
DORA — Reg. (UE) 2024/1773	Art. 4 — arreglos de gobernanza para el riesgo de terceros de TIC

P-04 ¿Están asignadas de manera documentada las responsabilidades y competencias para la cadena de suministro (RACI)?

Criticidad: Baja · Obligatoria en todos los niveles de criticidad (Baja, Media, Alta).

Justificación

La entidad necesita asignar todas las responsabilidades relacionadas con la cadena de suministro, de modo que no se adquieran servicios no deseados y que la supervisión continua de los proveedores tenga responsables claros. Las responsabilidades difusas — "alguien de TI" o "alguien de legal" — generan brechas en la debida diligencia e incidentes que no se gestionan de manera coherente.

Ejemplos e información adicional

Mantener una matriz tipo RACI que cubra, como mínimo, los puntos siguientes. La matriz debería revisarse cuando haya cambios organizacionales y al menos una vez al año.

- Quién está autorizado a firmar contratos de adquisición.
- Si existe un umbral por encima del cual se requiere la aprobación de la dirección para una nueva contratación.
- Quién es responsable de evaluar los contratos existentes y de asegurar que los nuevos contratos se registren en el sistema de gestión de licencias de la entidad.
- Quién valida la postura de seguridad del proveedor antes de la firma del contrato.
- Quién es el punto de contacto operativo con cada proveedor durante el contrato.
- Quién valida las notificaciones de incidentes recibidas de los proveedores.
- Quién autoriza los cambios de subencargados y los cambios de propiedad del proveedor.
- Quién aprueba la terminación del contrato y el plan de salida.

Mapeo

Marco	Referencia / cláusula
ISO/IEC 27036-2	Cláusula 6.2 — Roles y responsabilidades en las relaciones con los proveedores
ISO/IEC 27001:2022	Cláusulas 5.1, 5.3 — Compromiso de la dirección y roles
NIST SP 800-161 Rev. 1	Sección 2.3.3 — PMO de C-SCRM y roles

P-05 ¿Se incluye a todas las partes interesadas pertinentes en el proceso de contratación desde una etapa temprana?

Criticidad: Media · Obligatoria en las contrataciones de criticidad Media y Alta.

Justificación

Las nuevas contrataciones, especialmente las de sistemas de mayor envergadura, pueden generar amplias discusiones entre las partes interesadas. Esas discusiones pueden aportar perspectivas útiles que ayuden a los tomadores de decisiones a identificar al proveedor adecuado, pero también pueden causar inquietud entre los empleados, los clientes o las autoridades. Para prevenir problemas imprevistos, todas las partes interesadas pertinentes deberían incluirse de manera temprana y proactiva.

Ejemplos e información adicional

Las partes interesadas dependen del contexto de la entidad y de la contratación en cuestión.

- Personal de TI y de operaciones
- Oficiales de ciberseguridad / CISO
- Empleados (o sus representantes) y representantes sindicales
- Clientes y ciudadanos (cuando corresponda)
- Proveedores o suplidores existentes que puedan verse afectados
- Autoridades competentes y reguladores
- Entidades asociadas
- Asesores legales

Mapeo

Marco	Referencia / cláusula
ISO/IEC 27036-1	Cláusula 5 — Participación multidisciplinaria
DORA — Reg. (UE) 2024/1773	Tres líneas de defensa en el riesgo de terceros
NIST SP 800-161 Rev. 1	Sección 2.3.3 — Participación interfuncional

P-06 ¿Se planifica con antelación la integración del producto o servicio adquirido, incluidos los plazos de instalación, capacitación, transición e inicio de uso?

Criticidad: Baja · Obligatoria en todos los niveles de criticidad (Baja, Media, Alta).

Justificación

Los nuevos servicios o productos deberían integrarse con un plan, y no sin considerar todos los aspectos pertinentes. Un enfoque planificado ayuda a asegurar que la contratación pueda ejecutarse dentro del tiempo y el costo previstos, y reduce el margen para errores que afecten la ciberseguridad.

Ejemplos e información adicional

Un plan de integración debería incluir, como mínimo, las siguientes consideraciones:

- Momento de la firma del contrato
- Tiempo hasta que el servicio o producto esté listo para instalarse
- Plazo de instalación
- Plazo de capacitación del personal, incluida la capacitación en seguridad
- Período de transición si se reemplaza un sistema antiguo, incluida la transferencia de datos
- Momento de inicio del uso
- Decisiones estratégicas de política y de gestión adoptadas en cada hito
- Participación de las partes interesadas en cada hito

Mapeo

Marco	Referencia / cláusula
ISO/IEC 27036-2	Cláusula 7 — Inicio de la relación con el proveedor
NIST SP 800-161 Rev. 1	Sección sobre integración del ciclo de vida
Plantilla SCRM de CISA	P. 2.3 — Ciclo de vida de extremo a extremo

P-07 ¿Realiza la entidad evaluaciones de riesgo para los servicios y productos recién adquiridos?

Criticidad: Baja · Obligatoria en todos los niveles de criticidad (Baja, Media, Alta).

Justificación

Una evaluación de riesgos ayuda a identificar y reducir los riesgos para las operaciones del negocio de la entidad. Los riesgos son amenazas combinadas con su probabilidad de ocurrencia. Si la entidad utiliza un marco formal de gestión de riesgos, debería incorporar los nuevos proyectos de contratación a ese marco.

El estudio de ENISA de 2023 encontró que solo el 37 % de las organizaciones demuestra debida diligencia o evaluaciones de riesgo de sus proveedores, y que el 9 % no evalúa en absoluto el riesgo de la cadena de suministro — una brecha notable.

Ejemplos e información adicional

ISO/IEC 27005 es un marco de evaluación de riesgos enfocado en la ciberseguridad. NIST SP 800-30 es el equivalente estadounidense. El anexo práctico (howto) de estas directrices describe una metodología mínima de seis pasos.

Las amenazas a considerar para las nuevas contrataciones pueden incluir, entre otras:

- Falla del servicio en el tercero

- Fuga de información en el tercero (p. ej., Verkada 2021 — credenciales encontradas en línea dieron acceso a 150,000 cámaras de clientes)
- Vulnerabilidad de software en el producto adquirido (p. ej., Kaseya VSA 2021 — un zero-day utilizado para distribuir ransomware a los clientes gestionados)
- Propagación de código o software malicioso a través del proveedor (p. ej., SolarWinds 2020 — malware inyectado en el proceso de compilación de Orion)
- Compromiso de un subencargado
- Configuración incorrecta en el entorno del proveedor (p. ej., Codecov 2021 — un error en una imagen de Docker expuso credenciales, utilizadas para modificar un script bash de cara a los clientes)

Panorama de Amenazas de ENISA — caso ilustrativo: Verkada (marzo de 2021): credenciales presuntamente encontradas en línea (OSINT) dieron a los atacantes acceso a 150,000 cámaras de clientes. SolarWinds (2020) y Kaseya VSA (julio de 2021) son casos de referencia del patrón de ataque a la cadena de suministro.

Mapeo

Marco	Referencia / cláusula
ISO/IEC 27005	Gestión de riesgos de seguridad de la información
NIST SP 800-30	Guía para realizar evaluaciones de riesgo
NIST SP 800-161 Rev. 1	Apéndice C — Marco de exposición al riesgo
Buenas Prácticas de ENISA (2023)	Área 3.2 — Gestión de riesgos de la cadena de suministro

P-08 ¿Existe una política publicada de seguridad de las contrataciones aprobada por la alta dirección?

Criticidad: Baja · Obligatoria en todos los niveles de criticidad (Baja, Media, Alta).

Justificación

Una política hace explícitas las expectativas de la entidad, tanto internamente como frente a los oferentes. Favorece la coherencia en la toma de decisiones y brinda cobertura legal para rechazar ofertas que no cumplan los requisitos mínimos de ciberseguridad.

Ejemplos e información adicional

La política debería hacer referencia a estas Directrices como fuente de los requisitos mínimos, definir la clasificación por niveles de riesgo de los proveedores, listar las cláusulas modelo y definir las rutas de escalamiento. Debería ser aprobada al más alto nivel ejecutivo y publicarse, como mínimo, en un portal interno.

Mapeo

Marco	Referencia / cláusula
Directiva NIS2	Art. 21(2)(a) — políticas de análisis de riesgos y seguridad de los sistemas de información
ISO/IEC 27001:2022	Cláusula 5.2 — Política de seguridad de la información
Buenas Prácticas de ENISA (2023)	Área 3.1 — Política y marco
Plantilla SCRM de CISA	P. 4.3 — políticas a nivel de toda la empresa

P-09 ¿Existe un grupo multidisciplinario de gobernanza de las contrataciones (legal, TI/seguridad, compras, negocio)?

Criticidad: Alta · Obligatoria solo en las contrataciones de criticidad Alta.

Justificación

Las decisiones de ciberseguridad de la cadena de suministro atraviesan varias funciones — dimensiones legales, técnicas, financieras y operativas. Un grupo permanente, en lugar de consultas ad hoc, es el único mecanismo sostenible.

Ejemplos e información adicional

El grupo debería reunirse al menos trimestralmente y a demanda para decisiones sobre contrataciones críticas. Debería revisar el registro de riesgos de proveedores, aprobar las aceptaciones de riesgos relevantes y validar el uso de las cláusulas modelo.

Mapeo

Marco	Referencia / cláusula
ISO/IEC 27036-1	Panorama general — participación multidisciplinaria
DORA — Reg. (UE) 2024/1773	Disposiciones sobre el órgano de dirección
NIST SP 800-161 Rev. 1	Sección 2.3.3

P-10 ¿Mantiene la entidad un registro de riesgos de la cadena de suministro que se revisa periódicamente?

Criticidad: Media · Obligatoria en las contrataciones de criticidad Media y Alta.

Justificación

Un registro de riesgos de los proveedores — y no solo un registro de proveedores — es el instrumento operativo que traduce la política en decisiones cotidianas. Permite escalar los controles, priorizar el monitoreo y dar trazabilidad a las decisiones de aceptación de riesgos.

La Guía de Implementación Técnica de ENISA sobre el Reg. (UE) 2024/2690 detalla cómo los riesgos relacionados con los proveedores deberían alimentar las medidas generales de gestión de riesgos de la entidad.

Ejemplos e información adicional

El registro debería estar vinculado al proceso más amplio de gestión de riesgos de seguridad de la información de la entidad, pero ser lo suficientemente específico para capturar el riesgo proveedor por proveedor. Cada entrada debería incluir el proveedor,

el servicio/producto, el nivel de criticidad, el riesgo residual, el responsable del riesgo y la fecha de la próxima revisión.

Mapeo

Marco	Referencia / cláusula
Guía de Implementación Técnica de ENISA — Reg. (UE) 2024/2690	Sección sobre gestión de riesgos de seguridad de la cadena de suministro
ISO/IEC 27005	Gestión de riesgos de seguridad de la información
NIST SP 800-161 Rev. 1	Apéndice C — Marco de exposición al riesgo
Directiva NIS2	Art. 21(2)(d), Art. 22
Buenas Prácticas de ENISA (2023)	Área 3.2 — Gestión de riesgos de la cadena de suministro

10.2 Selección de proveedores y productos

La selección es la etapa en la que la entidad obtiene su información sobre el proveedor y fija las obligaciones contractuales. Las recomendaciones de esta sección cubren la exigibilidad legal, la debida diligencia técnica sobre el proveedor y el producto, los controles mínimos de ciberseguridad, las cláusulas contractuales y la integridad del producto. Se basan en las Buenas Prácticas de ENISA, el Panorama de Amenazas de ENISA sobre Ataques a la Cadena de Suministro (2021) — del cual se toman varios ejemplos basados en incidentes — el CRA de la UE, ISO/IEC 27036, la Plantilla SCRM para Proveedores de CISA y NIST SP 800-161 Rev. 1.

S-01 ¿Puede hacerse cumplir un contrato con el tercero en la jurisdicción desde la que este opera?

Criticidad: Baja · Obligatoria en todos los niveles de criticidad (Baja, Media, Alta).

Justificación

Al formalizar un contrato con un tercero, la entidad debería considerar si el contrato puede hacerse cumplir por vías legales. Esto es especialmente relevante en contratos con terceros que operan desde otra jurisdicción u otro país, y donde los regímenes de acceso gubernamental pueden prevalecer sobre la confidencialidad comercial.

Ejemplos e información adicional

Los asesores legales deberían revisar la elección de la ley aplicable, la elección del foro y la exigibilidad práctica frente a la estructura del grupo del proveedor. Cuando el proveedor forme parte de un grupo multinacional, debería exigirse una parte contratante establecida en la región.

Mapeo

Marco	Referencia / cláusula
ISO/IEC 27036-2	Cláusula 6.3 — Requisitos legales y regulatorios
DORA — Reg. (UE) 2024/1773	Disposiciones sobre arreglos contractuales y ley aplicable

Marco	Referencia / cláusula
Evaluación de Riesgos de Computación en la Nube de ENISA	Riesgos legales — jurisdicción
NIST SP 800-161 Rev. 1	Sección 3.4 — Jurisdicción legal extranjera

S-02 ¿Otorga el contrato a la entidad (o a su auditor designado o a la autoridad competente) derechos de auditoría sobre el proveedor y sus subencargados?

Criticidad: Baja · Obligatoria en todos los niveles de criticidad (Baja, Media, Alta).

Justificación

Sin derechos de auditoría, la entidad no tiene medios independientes para verificar que el proveedor realmente implementa los controles de seguridad que afirma tener. Los derechos de auditoría también hacen posibles las auditorías ordenadas por el regulador cuando la propia entidad está supervisada.

Las Buenas Prácticas de ENISA identifican los derechos de auditoría como una obligación de rutina que los clientes deberían esperar. La Plantilla SCRM de CISA (P. 7.9) convierte las auditorías programadas periódicamente en un punto independiente.

Ejemplos e información adicional

Los derechos de auditoría deberían cubrir: el derecho a recibir informes estándar de auditoría de terceros (p. ej., ISO/IEC 27001, SOC 2 Tipo II); el derecho a solicitar información adicional; el derecho de la entidad, de un auditor externo o de un regulador a realizar auditorías in situ o remotas con un preaviso razonable; y el derecho a auditar a los subencargados a través del proveedor.

El RTS de DORA 1773 ofrece un punto de referencia sólido para las cláusulas de auditoría del sector financiero; el mismo modelo puede utilizarse en otros sectores.

Mapeo

Marco	Referencia / cláusula
DORA — Reg. (UE) 2024/1773	Derechos de auditoría e inspección
ISO/IEC 27036-2	Cláusula 7 — Verificación del proveedor
Buenas Prácticas de ENISA (2023)	Área 3.3 — Gestión de las relaciones con los proveedores
Plantilla SCRM de CISA	P. 4.17, 7.9 — Auditoría y aseguramiento contractuales

S-03 ¿Están ubicadas en lugares seguros las instalaciones del tercero necesarias para el servicio o producto?

Criticidad: Media · Obligatoria en las contrataciones de criticidad Media y Alta.

Justificación

Los servicios en la nube y los servicios gestionados dependen de instalaciones físicas. La ubicación determina la exposición a desastres naturales, inestabilidad política, regímenes de acceso gubernamental y riesgos operativos. La falta de transparencia sobre las ubicaciones es una señal de alerta.

Ejemplos e información adicional

El proveedor debería divulgar las ubicaciones primarias y de recuperación ante desastres de las instalaciones utilizadas para prestar el servicio. La entidad debería evaluar: la estabilidad política, la exposición a desastres naturales, la existencia de un régimen de control de exportaciones o de acceso gubernamental, y la seguridad física del sitio (típicamente mediante informes ISO/IEC 27001 o SOC 2).

Panorama de Amenazas de ENISA — caso ilustrativo: Verkada (marzo de 2021): el servidor de producción del proveedor fue comprometido — el problema no fue la ubicación física, sino la falta de segmentación entre instalaciones.

Mapeo

Marco	Referencia / cláusula
Evaluación de Riesgos de Computación en la Nube de ENISA	Riesgos físicos y ambientales
ISO/IEC 27001:2022	Anexo A.7 — Controles físicos
Caja de Herramientas de la UE para la Cadena de Suministro de TIC	Escenarios de riesgo sobre localización de datos
Plantilla SCRM de CISA	P. 5.1-5.7 — Seguridad física

S-04 ¿Opera el tercero un Sistema de Gestión de Seguridad de la Información (SGSI) que cubra el servicio o producto adquirido?

Criticidad: Baja · Obligatoria en todos los niveles de criticidad (Baja, Media, Alta).

Justificación

Un SGSI demuestra que el proveedor gestiona la seguridad de la información como una actividad sistemática y no como correcciones ad hoc. La certificación ISO/IEC 27001 por un organismo acreditado es la forma de aseguramiento más ampliamente reconocida.

La entidad debería verificar que el producto o servicio adquirido esté efectivamente dentro del alcance certificado, ya que un SGSI puede cubrir solo ciertas áreas de una empresa. El estudio de ENISA de 2023 encontró que el 61 % de las organizaciones exige certificación de seguridad a sus proveedores, pero la verificación del alcance suele faltar.

Ejemplos e información adicional

La entidad debería solicitar el certificado, la Declaración de Aplicabilidad y el informe más reciente de la auditoría de seguimiento. Para los sectores con expectativas más estrictas, debería exigirse un aseguramiento equivalente o superior — SOC 2 Tipo II, certificaciones sectoriales, EUCC de la UE para productos, EUCS para servicios en la nube.

Mapeo

Marco	Referencia / cláusula
ISO/IEC 27001:2022	Norma completa
Ley de Ciberseguridad de la UE — Reg. (UE) 2019/881	Marco de certificación de ciberseguridad
Esquema EUCS de ENISA	Certificación de servicios en la nube
Esquema EUCC de ENISA	Certificación de productos TIC — Reg. de Ejecución (UE) 2024/482
Plantilla SCRM de CISA	P. 4.1, 4.2 — Certificación / marco

S-05 ¿Cuenta el tercero con un plan documentado de gestión de incidentes de ciberseguridad, que incluya obligaciones de notificación hacia los clientes?

Criticidad: **Media** · Obligatoria en las contrataciones de criticidad Media y Alta.

Justificación

En caso de un incidente de seguridad o de la detección de una vulnerabilidad, el proveedor debería contar con procedimientos de gestión de incidentes planificados de antemano. Esto reduce significativamente el tiempo de reacción y asegura que las entidades afectadas sean informadas y asesoradas sobre las acciones a tomar.

Mimecast (2021) mostró cómo una notificación tardía o incompleta del proveedor agrava el impacto: los clientes necesitaron días para descubrir que los certificados utilizados para autenticarse en sus inquilinos (tenants) de Microsoft 365 habían sido comprometidos. Las guías de respuesta preexistentes acortan esta brecha.

Ejemplos e información adicional

El plan debería estar documentado, ejercitado y compartido con la entidad en la medida necesaria. El proveedor debería designar un contacto de CSIRT o PSIRT y proporcionar sus datos. ISO/IEC 27035 y el Marco de Servicios PSIRT de FIRST.org son referencias útiles.

Panorama de Amenazas de ENISA — caso ilustrativo: Mimecast (enero de 2021): los atacantes utilizaron un certificado comprometido del proveedor para autenticarse en los inquilinos (tenants) de Microsoft 365 de los clientes — lo que subraya el valor de una divulgación rápida por parte del proveedor.

Mapeo

Marco	Referencia / cláusula
ISO/IEC 27035	Gestión de incidentes
Directiva NIS2	Art. 21(2)(b) — gestión de incidentes
Buenas Prácticas de ENISA (2023)	Área 3.3 — Obligaciones del proveedor en la gestión de incidentes
Plantilla SCRM de CISA	P. 4.25 — CSIRT y notificación a los clientes

S-06 ¿Ha proporcionado el proveedor una Lista de Materiales de Software (SBOM)?

Criticidad: Baja · Obligatoria en todos los niveles de criticidad (Baja, Media, Alta).

Justificación

Un SBOM es una lista legible por máquina de los componentes contenidos en un producto de software. Sin un SBOM, ni el proveedor ni la entidad pueden determinar rápidamente si el producto está afectado por una vulnerabilidad recién divulgada — como lo ilustró Log4Shell a nivel mundial.

El Reglamento de Ciberresiliencia de la UE establece el SBOM como una expectativa horizontal para los productos con elementos digitales. Los Elementos Mínimos de SBOM de CISA / NTIA constituyen una referencia operativa útil, y la Plantilla SCRM de CISA (P. 2.5) convierte la entrega del BOM en una verificación independiente del proveedor.

Ejemplos e información adicional

Exigir un SBOM en formato CycloneDX o SPDX al momento de la aceptación y en cada actualización mayor del producto. El SBOM debería cubrir el código propio del proveedor y todos los componentes de código abierto y de terceros incluidos. Integrar el SBOM en la gestión de vulnerabilidades de modo que, cuando se divulgue una nueva vulnerabilidad, la entidad pueda determinar en cuestión de horas qué productos desplegados están afectados.

Mapeo

Marco	Referencia / cláusula
Reglamento de Ciberresiliencia de la UE — Reg. (UE) 2024/2847	Anexo I, Parte II — Gestión de vulnerabilidades: SBOM en formato legible por máquina
Elementos Mínimos de SBOM de CISA / NTIA	Formato, profundidad y campos requeridos
Buenas Prácticas de ENISA (2023)	Área 3.4 — Gestión de vulnerabilidades — transparencia de la cadena de suministro de software
NIST SP 800-161 Rev. 1	Sección 2.5 — Intercambio de información y SBOM
Plantilla SCRM de CISA	P. 2.5 — Cobertura del BOM y seguimiento de cambios

S-07 ¿Se ha verificado que el servicio o producto adquirido no presenta vulnerabilidades de seguridad conocidas?

Criticidad: Baja · Obligatoria en todos los niveles de criticidad (Baja, Media, Alta).

Justificación

Antes de adquirir un servicio o producto, la entidad debería verificar que no existan vulnerabilidades de seguridad conocidas. La forma más sencilla es cotejar el SBOM (S-06) con las bases de datos de vulnerabilidades.

Independientemente de la verificación del SBOM, la entidad debería revisar los reportes sobre problemas de seguridad no resueltos — publicaciones de ciberseguridad, bases de datos de CVE, avisos de los fabricantes, CSIRT sectoriales.

Ejemplos e información adicional

Utilizar la búsqueda en CVE / NVD, OSS Index o los avisos de seguridad de GitHub (GitHub Security Advisories), o aplicar herramientas comerciales de análisis de composición de software (SCA) al SBOM. Rechazar los productos que dependan de componentes sin parches y sin un control compensatorio documentado.

Mapeo

Marco	Referencia / cláusula
Buenas Prácticas de ENISA (2023)	Área 3.4 — Gestión de vulnerabilidades
ISO/IEC 30111	Procesos de tratamiento de vulnerabilidades
Plantilla SCRM de CISA	P. 4.14, 4.22 — Identificación y escaneo de vulnerabilidades antes de la aceptación
NIST SSDF (SP 800-218)	Prácticas PO y PW

S-08 ¿Sigue el tercero un Ciclo de Vida de Desarrollo Seguro (SDL) y protege la integridad de su entorno de compilación (build pipeline)?

Criticidad: Baja · Obligatoria en todos los niveles de criticidad (Baja, Media, Alta).

Justificación

El desarrollo de software debería seguir procedimientos que consideren la seguridad del producto. Los desarrolladores que utilizan un SDL estandarizado producen menos versiones vulnerables. El Art. 21(3) de NIS2 exige explícitamente a las entidades tener en cuenta las prácticas de desarrollo seguro de sus proveedores.

El ataque a SolarWinds (2020) inyectó código malicioso en el proceso de compilación de Orion — lo que hace que la integridad del entorno de compilación (CISA SCRM P. 3.6, 3.7, 3.13) sea tan importante como el propio SDL. Codecov (2021) fue una vulneración similar del entorno de compilación. El análisis de ENISA encontró que el 66 % de los ataques se dirigió al código o a los procesos de los proveedores.

Ejemplos e información adicional

Evidencia: estándares de codificación segura, revisión por pares obligatoria, modelado de amenazas, pruebas de seguridad (SAST, DAST, escaneo de dependencias), capacitación en seguridad de los desarrolladores y un proceso formal de liberación / aprobación. ISO/IEC 27034, BSIMM, el SDL de Microsoft y NIST SP 800-218 (SSDF) son referencias comunes.

Controles del entorno de compilación: integridad del código fuente (commits firmados), compilaciones reproducibles, versiones firmadas, procedencia alineada con SLSA, acceso restringido a la infraestructura de compilación.

Panorama de Amenazas de ENISA — caso ilustrativo: SolarWinds Orion (diciembre de 2020): malware inyectado durante el proceso de compilación del proveedor; alrededor de 18,000 clientes recibieron la actualización comprometida. Codecov (abril de 2021): credenciales robadas de una imagen de Docker se utilizaron para modificar un script bash de cara a los clientes — el mismo patrón de compromiso del entorno de compilación.

Mapeo

Marco	Referencia / cláusula
Directiva NIS2	Art. 21(3) — prácticas de desarrollo seguro de los proveedores
Reglamento de Ciberresiliencia de la UE	Anexo I — requisitos de desarrollo seguro
ISO/IEC 27034	Seguridad de las aplicaciones
NIST SSDF (SP 800-218)	Marco de Desarrollo Seguro de Software (Secure Software Development Framework)
Plantilla SCRM de CISA	P. 3.6, 3.7, 3.10, 3.13 — Integridad del código y de la compilación
SLSA de Google	Supply chain Levels for Software Artifacts (Niveles de la cadena de suministro para artefactos de software)

S-09 ¿Se compromete el tercero a proporcionar actualizaciones de seguridad durante todo el período previsto de uso, con una Política de Divulgación de Vulnerabilidades publicada?

Criticidad: Baja · Obligatoria en todos los niveles de criticidad (Baja, Media, Alta).

Justificación

Si se identifica un problema de seguridad después de que un producto se considera fuera de su vida útil, la entidad puede verse obligada a operarlo en estado vulnerable. Las entidades deben seleccionar productos que recibirán actualizaciones de seguridad durante todo su período previsto de uso — esto debería especificarse en el contrato.

Una Política de Divulgación de Vulnerabilidades (VDP) publicada crea un canal seguro para que los investigadores de seguridad reporten vulnerabilidades de manera responsable. Los Arts. 13-14 del CRA de la UE imponen a los fabricantes obligaciones específicas en materia de gestión de vulnerabilidades y divulgación coordinada.

Ejemplos e información adicional

El proveedor debería divulgar: el período de soporte previsto y la fecha de fin de vida; el SLA de aplicación de parches para vulnerabilidades críticas; el canal para recibir avisos; y el punto de contacto de la VDP (típicamente un archivo security.txt o una página de seguridad dedicada).

La VDP del proveedor debería comprometerse a acusar recibo de los reportes dentro de un plazo declarado y definir el proceso de triaje, mitigación y divulgación coordinada.

Mapeo

Marco	Referencia / cláusula
Reglamento de Ciberresiliencia de la UE — Reg. (UE) 2024/2847	Arts. 13-14 — gestión de vulnerabilidades y actualizaciones de seguridad
ISO/IEC 29147	Divulgación de vulnerabilidades
ISO/IEC 30111	Procesos de tratamiento de vulnerabilidades

Marco	Referencia / cláusula
Buenas Prácticas de ENISA (2023)	Área 3.4 — Gestión de vulnerabilidades
Plantilla SCRM de CISA	P. 3.16 — PSIRT

S-10 ¿Proporciona el tercero portabilidad de los datos para prevenir la dependencia del proveedor (vendor lock-in)?

Criticidad: Baja · Obligatoria en todos los niveles de criticidad (Baja, Media, Alta).

Justificación

Muchos servicios y productos utilizan formatos de datos propietarios. Los datos creados con el servicio solo pueden visualizarse o editarse con ese servicio. Algunos servicios ni siquiera ofrecen una opción de exportación. En ese caso, los datos no pueden transferirse a otros servicios, lo que puede resultar en pérdida de datos si el servicio se retira de operación.

Ejemplos e información adicional

Todo servicio o producto debería ofrecer opciones de exportación. Como mínimo, debería ser posible obtener una exportación legible por humanos que pueda procesarse manualmente. Una mejor opción es una exportación legible por máquina en un formato abierto que otros productos puedan utilizar sin mucho esfuerzo. El contrato debería fijar el formato de exportación, la frecuencia de exportación y el plazo máximo de entrega.

La Ley de Datos de la UE (Reg. (UE) 2023/2854) introduce obligaciones de cambio de proveedor y portabilidad para los servicios de procesamiento de datos que pueden tomarse como referencia.

Mapeo

Marco	Referencia / cláusula
Guía de Implementación Técnica de ENISA — Reg. (UE) 2024/2690	Continuidad y portabilidad de los datos
Evaluación de Riesgos de Computación en la Nube de ENISA	Riesgos de dependencia (lock-in)
Ley de Datos de la UE — Reg. (UE) 2023/2854	Obligaciones de cambio de proveedor y portabilidad
ISO/IEC 19941 / 22123	Interoperabilidad y portabilidad en la nube

S-11 ¿Están validadas, vigentes y dentro del alcance del servicio adquirido las certificaciones de ciberseguridad del tercero?

Criticidad: Baja · Obligatoria en todos los niveles de criticidad (Baja, Media, Alta).

Justificación

Las certificaciones solo son significativas cuando están vigentes, dentro del alcance y emitidas por un organismo acreditado. Las certificaciones también deben certificar una materia pertinente — un certificado de gestión de calidad no sirve para

determinar la madurez en ciberseguridad, y un certificado de ciberseguridad que no cubre el centro de datos sino solo el área administrativa de un tercero es de utilidad limitada.

Ejemplos e información adicional

Validar el certificado con el organismo emisor o su registro público; verificar que el alcance cubra el servicio adquirido; revisar el informe más reciente de la auditoría de seguimiento / recertificación; y registrar la fecha de vencimiento para volver a verificar antes de la renovación del contrato.

Mapeo

Marco	Referencia / cláusula
Ley de Ciberseguridad de la UE — Reg. (UE) 2019/881	Marco europeo de certificación de ciberseguridad
EUCC de ENISA	Esquema basado en Common Criteria — Reg. (UE) 2024/482
EUCS de ENISA	Esquema para servicios en la nube
ISO/IEC 17021	Evaluación de la conformidad — requisitos de acreditación
Plantilla SCRM de CISA	P. 4.1 / 4.2 — atestación de terceros

S-12 ¿Ha proporcionado el proveedor su propia evaluación de riesgos del producto o servicio en cuestión, incluidos los riesgos residuales aceptados?

Criticidad: Media · Obligatoria en las contrataciones de criticidad Media y Alta.

Justificación

El proveedor ve riesgos que la entidad no puede ver — la arquitectura interna, el historial de vulnerabilidades, las dependencias de subencargados. Exigir la evaluación de riesgos del proveedor hace transparentes esos riesgos e informa la propia gestión de riesgos de la entidad.

Ejemplos e información adicional

El proveedor debería entregar una evaluación de riesgos resumida a la firma del contrato y en cada versión mayor, indicando los riesgos residuales aceptados por el proveedor y cualquier control compensatorio esperado de la entidad.

Mapeo

Marco	Referencia / cláusula
ISO/IEC 27036-3	Directrices para la cadena de suministro de TIC — lado del proveedor
Buenas Prácticas de ENISA (2023)	Área 3.2 — Gestión de riesgos de la cadena de suministro
Reglamento de Ciberresiliencia de la UE	Diseño basado en riesgos y evaluación de la conformidad
Plantilla SCRM de CISA	P. 2.3 — Implementación de la estrategia

S-13 ¿Está el personal del proveedor con acceso a los sistemas o datos de la entidad sujeto a una verificación de seguridad (verificación de antecedentes, referencias) proporcional al rol?

Criticidad: Media · Obligatoria en las contrataciones de criticidad Media y Alta.

Justificación

El riesgo interno en la organización del proveedor es un vector recurrente de incidentes — técnicos con privilegios, ingenieros de guardia, personal de soporte. Una verificación proporcional reduce la probabilidad de actores internos maliciosos sin imponer un costo desproporcionado.

La Plantilla SCRM de CISA, P. 6.3-6.5, exige explícitamente políticas de verificación de antecedentes para los propios empleados del proveedor, los proveedores del proveedor y cualquier subcontratista, con salvedades para las jurisdicciones donde esto no esté legalmente permitido.

Ejemplos e información adicional

La verificación debería ser proporcional a la clasificación de los datos y al nivel de acceso. Línea base típica: verificación de identidad, verificación del historial laboral y compromiso de confidencialidad. Para roles privilegiados o críticos: verificación de antecedentes penales (donde esté legalmente permitido), referencias y verificaciones periódicas.

Incorporación: documentada; cubre la capacitación en concienciación sobre seguridad y la entrega de activos. Desvinculación: documentada; cubre la remoción de accesos y la recuperación de activos.

Mapeo

Marco	Referencia / cláusula
ISO/IEC 27001:2022	Anexo A.6 — Controles sobre las personas
ISO/IEC 27036-2	Cláusulas de seguridad del personal
Plantilla SCRM de CISA	P. 6.1-6.6 — Seguridad del personal, incorporación, desvinculación
NIST SP 800-161 Rev. 1	Seguridad del personal en la cadena de suministro

S-14 ¿Están identificados y controlados contractualmente los subencargados / cuartas partes, con notificación de cambios?

Criticidad: Media · Obligatoria en las contrataciones de criticidad Media y Alta.

Justificación

La mayoría de los servicios modernos depende de subencargados. Una brecha en una cuarta parte puede propagarse hacia arriba en la cadena de suministro hasta la entidad, aun cuando la entidad no tenga una relación directa con esa parte. La tendencia regulatoria reciente (RTS de DORA 532, NIS2 Art. 22) consiste en hacer obligatorios la visibilidad y el control de las cuartas partes.

La Plantilla SCRM de CISA, P. 2.10, convierte la notificación de cambios de subcontratistas en una obligación independiente.

Ejemplos e información adicional

El contrato debería exigir: una lista actualizada de subencargados; la aprobación previa (o al menos la notificación con derecho de objeción) de los nuevos subencargados; el traslado de las obligaciones de seguridad de la entidad a los subencargados; y derechos de auditoría que se extiendan a los subencargados a través del proveedor principal.

Mapeo

Marco	Referencia / cláusula
DORA — Reg. (UE) 2025/532	RTS sobre subcontratación
Directiva NIS2	Art. 21(2)(d) y Art. 22
ISO/IEC 27036-2	Cadena de suministro extendida
Plantilla SCRM de CISA	P. 2.10 — Notificación de cambios de subcontratistas

S-15 ¿Exige el contrato la notificación de los cambios de propiedad, control o ubicación del proveedor?

Criticidad: Media · Obligatoria en las contrataciones de criticidad Media y Alta.

Justificación

Las fusiones, las adquisiciones, los cambios de control o la reubicación de las operaciones pueden cambiar sustancialmente el perfil de riesgo de un proveedor — por ejemplo, al someterlo a una jurisdicción, un régimen de sanciones o un régimen de acceso gubernamental diferentes.

Ejemplos e información adicional

El contrato debería exigir la notificación anticipada de: los cambios de propiedad por encima de un umbral definido (p. ej., 25 %); los cambios en el país de constitución o el país de operación; los cambios en el país de almacenamiento de los datos. La entidad debería conservar el derecho contractual de rescindir sin penalidad si el cambio resulta inaceptable.

Mapeo

Marco	Referencia / cláusula
DORA — Reg. (UE) 2024/1773	Arreglos contractuales: cambio de control
Buenas Prácticas de ENISA (2023)	Área 3.3 — Gestionar los cambios en los acuerdos con los proveedores
Caja de Herramientas de la UE para la Cadena de Suministro de TIC	Dependencia estratégica

S-16 ¿Se incluyen controles mínimos de ciberseguridad en las especificaciones de la licitación y se ponderan en la evaluación?

Criticidad: Baja · Obligatoria en todos los niveles de criticidad (Baja, Media, Alta).

Justificación

Si la ciberseguridad no es un criterio de evaluación puntuado, los proveedores competirán solo por precio y cronograma, y ganará la oferta insegura más barata. Incorporar controles mínimos y una puntuación de seguridad en la matriz de evaluación cambia ese incentivo.

Ejemplos e información adicional

Las especificaciones de la licitación deberían incluir una sección clara de requisitos mínimos (cumple / no cumple) y una sección de ciberseguridad puntuada. La sección de requisitos mínimos debería hacer referencia a estas directrices y dejar explícito que cualquier incumplimiento de los puntos obligatorios descalifica la oferta. La sección puntuada debería premiar a los proveedores con mayor aseguramiento, certificaciones más amplias y prácticas de SDL más transparentes.

Mapeo

Marco	Referencia / cláusula
Buenas Prácticas de ENISA (2023)	Área 3.5 — Calidad de los productos y las prácticas
Directivas de contratación pública de la UE	Uso de criterios de adjudicación cualitativos
ISO/IEC 27036-2	Cláusula sobre selección de proveedores

S-17 Para las adquisiciones de hardware, ¿se abastece el proveedor únicamente de fabricantes de equipos originales (OEM) o revendedores licenciados, con controles antifalsificación y embalajes que evidencien cualquier apertura o manipulación?

Criticidad: Alta · Obligatoria solo en las contrataciones de criticidad Alta.

Justificación

El hardware falsificado es un vector de ataque documentado — componentes modificados, embalajes manipulados o firmware falso entran a la cadena de suministro a través de revendedores no autorizados. La Plantilla SCRM de CISA, P. 5.10 y P. 2.6 / 2.7, cubre el abastecimiento exclusivo de OEM, el BOM controlado y la cadena de custodia.

Ejemplos e información adicional

Exigir: abastecimiento exclusivo de OEM o revendedores autorizados para los componentes clave; embalajes que evidencien cualquier apertura o manipulación; BOM controlado y documentación de cadena de custodia en tránsito; procesos del lado del proveedor para detectar y desechar piezas falsificadas.

Mapeo

Marco	Referencia / cláusula
Plantilla SCRM de CISA	P. 2.6, 2.7, 5.10 — OEM/revendedores autorizados, BOM, detección de manipulación, prevención de falsificaciones
NIST SP 800-161 Rev. 1	Procedencia e integridad
ISO/IEC 27036-2	Cláusula sobre integridad del hardware

S-18 ¿Protege el proveedor la integridad del código, del entorno de compilación y de la distribución de las versiones de software (versiones firmadas, entornos de compilación controlados, ausencia de cambios no autorizados)?

Criticidad: Alta · Obligatoria solo en las contrataciones de criticidad Alta.

Justificación

Los ataques a SolarWinds y Codecov comprometieron ambos el entorno de compilación del proveedor y utilizaron el propio canal de distribución del proveedor para enviar código malicioso a los clientes. La integridad del entorno de compilación es, por tanto, distinta de las prácticas de SDL y amerita su propia verificación.

La Plantilla SCRM de CISA, P. 3.6, 3.7 y 3.13, cubre explícitamente la protección del código frente a cambios no autorizados, la verificación de la integridad de las versiones de software y los procesos endurecidos de compilación.

Ejemplos e información adicional

Evidencia: firma de código, compilaciones reproducibles, acceso restringido a la infraestructura de compilación, auditoría del entorno de compilación, lista de materiales de software al momento de la liberación, alineación opcional con los niveles SLSA de Google.

Panorama de Amenazas de ENISA — caso ilustrativo: SolarWinds Orion (2020) — código malicioso inyectado en el proceso de compilación del proveedor. Codecov (2021) — script bash modificado utilizando credenciales extraídas de una imagen de Docker. Ambos ataques eludieron los controles del lado del cliente porque se originaron dentro del canal de distribución del proveedor.

Mapeo

Marco	Referencia / cláusula
Plantilla SCRM de CISA	P. 3.6, 3.7, 3.10, 3.13 — Integridad del código y del proceso de compilación
SLSA de Google	Supply chain Levels for Software Artifacts (Niveles de la cadena de suministro para artefactos de software)
NIST SSDF (SP 800-218)	Práctica PS — Protect the Software [Proteger el software]
Buenas Prácticas de ENISA (2023)	Área 3.5 — Calidad de los productos

10.3 Operaciones

Las operaciones constituyen la fase más larga de la relación con el proveedor. Las recomendaciones de esta sección cubren el monitoreo continuo de riesgos, las operaciones conjuntas, la capacitación, el endurecimiento de la configuración, los controles de identidad y acceso, la segmentación, la aplicación de parches y la gobernanza del personal del lado del proveedor. Muchas brechas originadas en proveedores ocurrieron no porque el contrato fuera débil, sino porque la relación no se gestionaba activamente.

O-01 ¿Se reevalúan el riesgo del proveedor y su postura de ciberseguridad al menos una vez al año y ante cambios relevantes?

Criticidad: Media · Obligatoria en las contrataciones de criticidad Media y Alta.

Justificación

Una evaluación inicial de riesgos antes de adquirir un nuevo servicio no basta para asegurar la seguridad a lo largo del tiempo. El riesgo de ciberseguridad necesita evaluarse de forma periódica. Una cadencia habitual es anual, más ante cambios relevantes (incidente notificado, cambio de control, cambio de criticidad).

Ejemplos e información adicional

Utilizar el mismo Cuestionario para Proveedores empleado en la selección, de modo que los cambios sean visibles. Actualizar el registro de riesgos de proveedores como resultado.

Mapeo

Marco	Referencia / cláusula
DORA — Reg. (UE) 2024/1774	Monitoreo periódico de los terceros de TIC
ISO/IEC 27036-2	Monitoreo continuo de la relación
Buenas Prácticas de ENISA (2023)	Área 3.3 — Monitoreo continuo
NIST SP 800-161 Rev. 1	Monitoreo continuo

O-02 ¿Se comparte información sobre amenazas de ciberseguridad e incidentes entre la entidad y el tercero?

Criticidad: Media · Obligatoria en las contrataciones de criticidad Media y Alta.

Justificación

Cuando una amenaza de ciberseguridad se hace conocida, compartirla aumenta la seguridad de ambas partes. La información sobre amenazas incluye incidentes, aumento de ataques (p. ej., campañas de phishing dirigidas) y nuevas vulnerabilidades que afecten el software utilizado por cualquiera de las partes.

Ejemplos e información adicional

El contrato debería definir qué categorías de información se compartirán (vulnerabilidades que afecten el producto, indicadores de compromiso observados por el proveedor, actividad sospechosa dirigida a la entidad), el canal (p. ej., MISP, correo seguro, portal) y la cadencia. Deberían abordarse la confidencialidad y la protección de la inteligencia compartida.

Mapeo

Marco	Referencia / cláusula
Directiva NIS2	Art. 29 — arreglos voluntarios de intercambio de información de ciberseguridad
Buenas Prácticas de ENISA (2023)	Área 3.3 — Intercambio de información

Marco	Referencia / cláusula
ISO/IEC 27010	Gestión de seguridad de la información para comunicaciones intersectoriales e interorganizacionales

O-03 ¿Están capacitados los administradores para asegurar la operación segura del servicio o producto adquirido, incluida la configuración relevante para la seguridad?

Criticidad: Baja · Obligatoria en todos los niveles de criticidad (Baja, Media, Alta).

Justificación

La configuración incorrecta de los servicios en la nube y gestionados es, de manera consistente, una de las principales causas raíz de las brechas. Los administradores capacitados son el control preventivo más costo-efectivo. La P. 4.16 de CISA SCRM convierte la capacitación en ciberseguridad de los administradores en una obligación independiente del proveedor.

Ejemplos e información adicional

El contrato debería incluir la capacitación inicial y una cadencia de actualización después de las versiones mayores. La capacitación debería cubrir la configuración de seguridad, la gestión de identidad y acceso, el registro (logging) y el monitoreo, y el proceso de respuesta a incidentes del proveedor. Dar seguimiento al cumplimiento de la capacitación.

- Operaciones criptográficas
- Gestión de identidad y acceso
- Configuración de red
- Gestión de parches
- Estrategia de respaldos

Mapeo

Marco	Referencia / cláusula
ISO/IEC 27001:2022	Anexo A.6.3 — Concienciación y capacitación
Buenas Prácticas de ENISA (2023)	Área 3.3 — Concienciación del personal
CIS Controls v8	Control 14 — Capacitación en Concienciación y Habilidades de Seguridad
Plantilla SCRM de CISA	P. 4.16 — Capacitación en ciberseguridad para administradores

O-04 ¿Están capacitados los usuarios finales en los aspectos sensibles para la seguridad del servicio o producto adquirido?

Criticidad: Baja · Obligatoria en todos los niveles de criticidad (Baja, Media, Alta).

Justificación

En muchos servicios o productos no solo los administradores, sino también los usuarios regulares, pueden realizar operaciones sensibles para la seguridad — compartir o editar datos del negocio, cambiar ciertas configuraciones que pueden exponer o alterar datos de maneras no deseadas.

Ejemplos e información adicional

El proveedor debería proporcionar material estándar de capacitación para usuarios finales, y la entidad debería integrar el producto del proveedor en su programa general de concienciación. Las simulaciones de phishing deberían incluir el producto del proveedor cuando sea pertinente.

- Intercambio de datos y exposición a terceros
- Alteración o eliminación de datos de manera no recuperable
- Activación de funciones con facturación adicional automática
- Carga no deseada de datos a servidores de terceros

Mapeo

Marco	Referencia / cláusula
ISO/IEC 27001:2022	Anexo A.6.3
Directiva NIS2	Art. 21(2)(g) — prácticas básicas de ciberhigiene y capacitación
Buenas Prácticas de ENISA (2023)	Área 3.3 — Concienciación del personal

O-05 ¿Está la configuración del servicio o producto adquirido endurecida conforme a una línea base definida y verificada por una persona distinta de la que la configuró?

Criticidad: Baja · Obligatoria en todos los niveles de criticidad (Baja, Media, Alta).

Justificación

Las configuraciones predeterminadas suelen estar optimizadas para la facilidad de instalación, no para la seguridad. Una línea base de endurecimiento documentada, alineada con las recomendaciones del proveedor y con referentes reconocidos, cierra debilidades conocidas. La configuración debería verificarse a intervalos regulares y después de cada actualización, y ser revisada por una persona distinta para evitar omisiones involuntarias.

Ejemplos e información adicional

Adoptar la guía de endurecimiento del proveedor, el CIS Benchmark pertinente o una línea base validada internamente. Dar seguimiento a las desviaciones de configuración y remediarlas. Cuando el servicio adquirido sea configurado por el proveedor, el contrato debería obligarlo a aplicar una línea base definida.

- Operaciones criptográficas
- Gestión de identidad y acceso
- Configuración de red
- Gestión de parches
- Estrategia de respaldos

Mapeo

Marco	Referencia / cláusula
CIS Benchmarks	Líneas base de configuración por tecnología
Buenas Prácticas de ENISA (2023)	Área 3.5 — Calidad de los productos y las prácticas
NIST SP 800-53 Rev. 5	Familia CM — Gestión de la Configuración
Plantilla SCRM de CISA	P. 3.15, 4.19 — Seguridad por defecto y endurecimiento

O-06 ¿Se realizan respaldos con regularidad, se almacenan de forma independiente del proveedor y pueden restaurarse sin el proveedor?

Criticidad: Baja · Obligatoria en todos los niveles de criticidad (Baja, Media, Alta).

Justificación

Los datos pueden perderse por fallas de hardware, eliminación accidental o ataques de ransomware. Una estrategia sólida de respaldos es necesaria para restaurar los datos. Los respaldos almacenados únicamente en la infraestructura o bajo el control exclusivo del proveedor son inútiles cuando el proveedor es la fuente de la interrupción.

Ejemplos e información adicional

Los respaldos deberían realizarse al menos diariamente, almacenarse fuera de la infraestructura y del control exclusivo del proveedor, en un formato que pueda restaurarse sin las herramientas del proveedor, y probarse al menos una vez al año. Las claves de cifrado deberían estar en poder de la entidad. Si el proveedor no ofrece respaldos automáticos, debería implementarse y auditarse un procedimiento manual fijo.

Mapeo

Marco	Referencia / cláusula
Directiva NIS2	Art. 21(2)(c) — continuidad del negocio
Evaluación de Riesgos de Computación en la Nube de ENISA	Dependencia (lock-in) / continuidad
CIS Controls v8	Control 11 — Recuperación de Datos
ISO/IEC 27031	Preparación de las TIC para la continuidad del negocio

O-07 ¿Están claramente asignadas las responsabilidades operativas entre la entidad y el tercero (RACI)?

Criticidad: Media · Obligatoria en las contrataciones de criticidad Media y Alta.

Justificación

Según el producto o servicio, la administración puede ser responsabilidad de la entidad, del tercero, o compartida. Para asegurar que ningún área de administración quede sin atender, todas las responsabilidades deben asignarse con claridad. La

desalineación es una causa raíz frecuente de fallas en la gestión de accesos (p. ej., cuentas de exempleados que permanecen habilitadas porque cada parte creía que la otra era responsable de deshabilitarlas).

Ejemplos e información adicional

Utilizar una matriz RACI que cubra los puntos siguientes. Revisarla ante cambios en el servicio y al menos una vez al año.

- Parches
- Configuraciones de seguridad
- Gestión de identidad y acceso
- Configuración
- Manejo de datos
- (Des)activación de funciones y complementos (plug-ins)
- Registro (logging) y monitoreo
- Pasos de respuesta a incidentes

Mapeo

Marco	Referencia / cláusula
ISO/IEC 27036-2	Responsabilidades operativas
Buenas Prácticas de ENISA (2023)	Área 3.3 — Titularidad operativa
Plantilla SCRM de CISA	P. 4.15 — Control de acceso a la red / basado en roles

O-08 ¿Se da seguimiento a los contratos (y licencias), se reevalúan y se renuevan (o se cancelan formalmente) de manera periódica?

Criticidad: **Media** · Obligatoria en las contrataciones de criticidad Media y Alta.

Justificación

Los contratos suelen tener una duración limitada o renovación automática. Todos los contratos de adquisición deberían ser objeto de seguimiento para asegurar que ningún producto o servicio quede inutilizable porque las licencias venzan inesperadamente, y para evitar renovaciones automáticas no deseadas de contratos que la entidad desea cancelar.

Ejemplos e información adicional

Establecer un procedimiento fijo para evaluar los contratos existentes de manera periódica. Dar seguimiento a las fechas clave: fin del plazo, fecha de activación de la renovación automática, período de preaviso, fin del período de soporte del proveedor.

Mapeo

Marco	Referencia / cláusula
ISO/IEC 27036-2	Gestión de la relación

Marco	Referencia / cláusula
Buenas Prácticas de ENISA (2023)	Área 3.3 — Gestionar los cambios

O-09 ¿Se aplican controles de identidad y acceso al personal de terceros (cuentas nominativas, MFA, elevación JIT, revisión periódica, sin acceso privilegiado permanente)?

Criticidad: Baja · Obligatoria en todos los niveles de criticidad (Baja, Media, Alta).

Justificación

El acceso privilegiado permanente del personal del proveedor es un vector de compromiso común. El acceso nominativo, limitado en el tiempo y protegido con MFA, con registro de actividad, reduce sustancialmente este riesgo. El incidente de Verkada ilustró cómo la ausencia de estos controles permitió a un actor externo acceder a consolas privilegiadas de gestión de videovigilancia.

Ejemplos e información adicional

Implementar: cuentas nominativas (sin cuentas compartidas) para el personal del proveedor; autenticación multifactor; elevación just-in-time para las acciones privilegiadas cuando sea técnicamente factible; grabación de sesiones para las actividades de alto riesgo; revisión trimestral de accesos.

Panorama de Amenazas de ENISA — caso ilustrativo: Verkada (marzo de 2021) — el acceso privilegiado disponible de forma remota sin controles fuertes permitió el acceso a 150,000 cámaras de clientes.

Mapeo

Marco	Referencia / cláusula
Directiva NIS2	Art. 21(2)(i) — políticas de control de acceso
Guía de Implementación Técnica de ENISA — Reg. (UE) 2024/2690	Sección de identidad y acceso
CIS Controls v8	Controles 5, 6 — Gestión de cuentas y accesos
ISO/IEC 27001:2022	Anexo A.5.15-5.18 — Control de acceso
Plantilla SCRM de CISA	P. 4.15 — Control de acceso a la red

O-10 ¿Está el servicio o producto adquirido segmentado a nivel de red del resto del entorno de la entidad, con listas de permitidos explícitas de entrada y salida?

Criticidad: Alta · Obligatoria solo en las contrataciones de criticidad Alta.

Justificación

La segmentación de red limita el movimiento lateral tras un compromiso — tanto desde el proveedor hacia la entidad como a la inversa. Es una de las medidas más efectivas contra el patrón de ataque a la cadena de suministro en el que un componente confiable del proveedor se convierte en el punto de entrada.

En el caso de SolarWinds, los clientes que segmentaron el tráfico saliente de Orion limitaron la exfiltración de manera significativa en comparación con los que permitieron un acceso saliente amplio desde el servidor de gestión.

Ejemplos e información adicional

Desplegar el producto del proveedor en un segmento de red dedicado con listas de permitidos explícitas de entrada y salida. Cuando el proveedor requiera conectividad hacia el entorno de la entidad, permitir a nivel de host y puerto, no a nivel de rango de IP. Terminar la conectividad cuando no sea necesaria.

Panorama de Amenazas de ENISA — caso ilustrativo: SolarWinds (2020) — las entidades que restringieron la conectividad saliente de Orion limitaron el impacto del implante.

Mapeo

Marco	Referencia / cláusula
CIS Controls v8	Control 12 — Gestión de la Infraestructura de Red
NIST SP 800-207	Arquitectura de Confianza Cero (Zero Trust)
Buenas Prácticas de ENISA (2023)	Área 3.5 — Defensa en profundidad
ISO/IEC 27001:2022	Anexo A.8.20-8.22 — Controles de red
Plantilla SCRM de CISA	P. 4.19 — Segmentación de red / IDS

O-11 ¿Está acordada contractualmente y monitoreada la gestión de parches y actualizaciones de seguridad?

Criticidad: Baja · Obligatoria en todos los niveles de criticidad (Baja, Media, Alta).

Justificación

El Art. 13 del CRA de la UE establece obligaciones para los fabricantes en materia de actualizaciones de seguridad durante todo el período de soporte. La entidad, por su parte, debe asegurar que esas actualizaciones lleguen efectivamente al producto desplegado dentro de un plazo definido.

Ejemplos e información adicional

El contrato debería especificar: el compromiso del proveedor de proporcionar actualizaciones de seguridad durante todo el período previsto de uso, el tiempo máximo para publicar un parche para vulnerabilidades críticas, la obligación de la entidad de desplegar los parches dentro de una ventana definida y las consecuencias de incumplir esas ventanas.

Mapeo

Marco	Referencia / cláusula
Reglamento de Ciberresiliencia de la UE — Reg. (UE) 2024/2847	Art. 13 — obligaciones de actualizaciones de seguridad

Marco	Referencia / cláusula
Directiva NIS2	Art. 21(2)(e) — seguridad en la adquisición, el desarrollo y el mantenimiento de redes y sistemas de información
Guía de Implementación Técnica de ENISA — Reg. (UE) 2024/2690	Sección de gestión de parches
CIS Controls v8	Control 7 — Gestión Continua de Vulnerabilidades
Plantilla SCRM de CISA	P. 4.23 — gestión de parches

O-12 ¿Existe un Código de Conducta que vincule al proveedor y a sus subcontratistas en materia de seguridad, privacidad y confidencialidad?

Criticidad: Media · Obligatoria en las contrataciones de criticidad Media y Alta.

Justificación

Un Código de Conducta, formalmente aceptado por el personal del proveedor y los subproveedores, hace explícitas las expectativas y facilita su exigibilidad. La P. 6.13 de CISA SCRM lo convierte en un control independiente.

Ejemplos e información adicional

El Código de Conducta debería estar disponible y visible para los empleados, proveedores y subcontratistas, mantenerse actualizado y acompañarse de capacitación. Debería designarse un punto de contacto para preguntas / violaciones.

Mapeo

Marco	Referencia / cláusula
Plantilla SCRM de CISA	P. 6.13 — Código de Conducta
ISO/IEC 27001:2022	Anexo A.5 — Políticas organizacionales

10.4 Gestión de vulnerabilidades

Continuamente se descubren vulnerabilidades en los productos y servicios de los que depende la entidad. Las Buenas Prácticas de ENISA identifican la gestión de vulnerabilidades como una de las cinco áreas de enfoque de la ciberseguridad de la cadena de suministro, distinta de la gestión de incidentes: una vulnerabilidad se convierte en incidente solo si es explotada. Las recomendaciones de esta sección cubren el lado del proveedor (PSIRT, análisis formal de vulnerabilidades y debilidades, análisis de causa raíz, calificación y política de mantenimiento basada en riesgos, notificación a los clientes) y el lado de la entidad (gestión interna de vulnerabilidades con monitoreo de SBOM, prueba de parches y reversión, participación en la divulgación coordinada de vulnerabilidades).

V-01 ¿Opera el tercero un Equipo de Respuesta a Incidentes de Seguridad de Productos (PSIRT) con un proceso documentado para evaluar, priorizar y remediar las vulnerabilidades reportadas?

Criticidad: Baja · Obligatoria en todos los niveles de criticidad (Baja, Media, Alta).

Justificación

Un PSIRT es la unidad operativa que convierte un reporte de vulnerabilidad en una corrección y un aviso. Sin un PSIRT — o con uno que carezca de criterios documentados de triaje — las vulnerabilidades quedan sin tratar y los clientes permanecen a oscuras.

Las Buenas Prácticas de ENISA (Área 3.4) y CISA SCRM §3.16 tratan la existencia de una función equivalente a un PSIRT como una expectativa de línea base para cualquier proveedor de productos o servicios digitales. El Marco de Servicios PSIRT de FIRST.org ofrece un modelo de lo que la función debería cubrir.

Ejemplos e información adicional

Evidencia que el proveedor debería aportar: estatuto del PSIRT o equivalente, punto de contacto designado (a menudo mediante security.txt), SLA de triaje, matriz de severidad y estadísticas del último año sobre el tiempo de corrección por nivel de severidad.

El PSIRT debería evaluar, priorizar y remediar las vulnerabilidades, asegurar que las correcciones se publiquen dentro de una ventana proporcional a la severidad y coordinar la divulgación con quienes las reportan.

Mapeo

Marco	Referencia / cláusula
Buenas Prácticas de ENISA (2023)	Área 3.4 — Gestión de vulnerabilidades: monitoreo, calificación, tratamiento, notificación a los clientes
Marco de Servicios PSIRT de FIRST.org	Definiciones de funciones y madurez
ISO/IEC 30111	Procesos de tratamiento de vulnerabilidades
Plantilla SCRM de CISA	P. 3.16 — Reporte y Respuesta a Incidentes de Seguridad de Productos (PSIRT)
Reglamento de Ciberresiliencia de la UE	Art. 13 — Gestión de vulnerabilidades por el fabricante

V-02 ¿Realiza el tercero un análisis formal de vulnerabilidades y debilidades en cada versión (SAST, DAST, análisis de composición de software, fuzzing)?

Criticidad: Media · Obligatoria en las contrataciones de criticidad Media y Alta.

Justificación

El análisis de vulnerabilidades previo a la liberación es el punto más barato para corregir problemas. Los proveedores sin un programa documentado descubrirán las mismas clases de errores una y otra vez — y los clientes pagarán el costo operativo.

CISA SCRM §3.14 lo convierte en un control independiente del proveedor, distinto del SDL en sentido amplio (S-08), y pregunta si el análisis está automatizado y si el código ejecutable se prueba antes de la liberación. La práctica PW del NIST SSDF (Produce Well-Secured Software: producir software bien protegido) cubre el mismo terreno.

Ejemplos e información adicional

Evidencia: lista de herramientas (p. ej., Semgrep / SonarQube para SAST, OWASP ZAP / Burp para DAST, Dependency-Check / Snyk para SCA, AFL / libFuzzer para fuzzing), la política de bloqueo (qué severidades impiden una liberación) y estadísticas agregadas de hallazgos cerrados antes de la liberación.

Mapeo

Marco	Referencia / cláusula
Buenas Prácticas de ENISA (2023)	Área 3.4 — Gestión de vulnerabilidades
NIST SSDF (SP 800-218)	Práctica PW — Produce Well-Secured Software [Producir software bien protegido]
Plantilla SCRM de CISA	P. 3.14 — Análisis formal de vulnerabilidades y debilidades
ISO/IEC 27034	Seguridad de las aplicaciones
Reglamento de Ciberresiliencia de la UE	Anexo I — diseño y desarrollo seguros

V-03 ¿Realiza el tercero un análisis de causa raíz de las vulnerabilidades divulgadas e incorpora las lecciones aprendidas en su SDL, sus herramientas y su capacitación?

Criticidad: Media · Obligatoria en las contrataciones de criticidad Media y Alta.

Justificación

Corregir una vulnerabilidad es necesario pero no suficiente. Si la causa subyacente — un patrón ausente en el modelo de amenazas, una clase de error que el análisis estático no detecta, una brecha de proceso — no se aborda, el mismo defecto reaparecerá en la próxima versión.

CISA SCRM §3.17 pregunta explícitamente a los proveedores si se realiza un análisis de causa raíz y si este informa las actualizaciones del proceso de desarrollo seguro, las herramientas y la capacitación.

Ejemplos e información adicional

Evidencia: un ejemplo de análisis post mortem de una vulnerabilidad divulgada recientemente, que muestre la causa raíz, las acciones correctivas en el SDL y el cierre de esas acciones; una métrica de clases de vulnerabilidades repetidas año tras año.

Mapeo

Marco	Referencia / cláusula
Buenas Prácticas de ENISA (2023)	Área 3.4 — Mejora continua de la gestión de vulnerabilidades
Plantilla SCRM de CISA	P. 3.17 — Análisis de causa raíz que alimenta el SDL
NIST SSDF (SP 800-218)	Práctica RV — Respond to Vulnerabilities [Responder a las vulnerabilidades]

V-04 ¿Utiliza el tercero un sistema documentado de calificación de vulnerabilidades (p. ej., CVSS) y una política de mantenimiento / aplicación de parches basada en riesgos?

Criticidad: Baja · Obligatoria en todos los niveles de criticidad (Baja, Media, Alta).

Justificación

Tratar todas las vulnerabilidades por igual es ineficiente y lento. Un sistema de calificación documentado (CVSS es el estándar de facto) y una política de mantenimiento que asocie la severidad con el tiempo de corrección y con las obligaciones de comunicación permiten decisiones consistentes y defendibles.

Las Buenas Prácticas de ENISA §3.4 exigen explícitamente el análisis de riesgos de las vulnerabilidades mediante un sistema de calificación de vulnerabilidades y políticas de mantenimiento para el tratamiento de las vulnerabilidades identificadas según el riesgo.

Ejemplos e información adicional

Evidencia: la política en sí (bandas de severidad, objetivos de tiempo de corrección por banda, disparadores de notificación a los clientes) y los factores ambientales de CVSS que aplica el proveedor. La política también debería contemplar las vulnerabilidades en componentes de terceros incorporados a través del SBOM (S-06).

Mapeo

Marco	Referencia / cláusula
Buenas Prácticas de ENISA (2023)	Área 3.4 — Análisis de riesgos con CVSS, políticas de mantenimiento
CVSS de FIRST.org	Sistema Común de Calificación de Vulnerabilidades
Plantilla SCRM de CISA	P. 3.16.1, 4.14 — Evaluación, priorización y remediación de vulnerabilidades
ISO/IEC 30111	Procesos de tratamiento de vulnerabilidades

V-05 ¿Cuenta el tercero con un proceso documentado y una cadencia para notificar a la entidad las vulnerabilidades que afecten el producto o servicio adquirido?

Criticidad: Baja · Obligatoria en todos los niveles de criticidad (Baja, Media, Alta).

Justificación

Un parche publicado sin notificación es invisible para la mayoría de los clientes. El proveedor debe contar con un proceso de notificación proactiva, con una cadencia y un contenido suficientes para el programa de gestión de vulnerabilidades de la entidad.

Las Buenas Prácticas de ENISA §3.4 incluyen los "procesos para informar a los clientes" como línea base. CISA SCRM §4.21 / §4.25 cubren las prácticas de detección de incidentes y el proceso del proveedor para notificar a los clientes cuando un producto o servicio se ve afectado.

Ejemplos e información adicional

Evidencia: la cadencia de avisos del proveedor (p. ej., mensual o por severidad), el canal (correo firmado, RSS, portal de clientes), el contenido (CVE, CVSS, versiones afectadas,

estado de explotación, mitigación) y el SLA de notificación proactiva para los avisos críticos.

Mapeo

Marco	Referencia / cláusula
Buenas Prácticas de ENISA (2023)	Área 3.4 — Procesos para informar a los clientes
Plantilla SCRM de CISA	P. 4.21, 4.25 — Notificación a los clientes en caso de impacto
ISO/IEC 29147	Divulgación coordinada de vulnerabilidades
Reglamento de Ciberresiliencia de la UE	Art. 14 — Divulgación coordinada de vulnerabilidades

V-06 ¿Mantiene la entidad su propio programa de gestión de vulnerabilidades que cubra el software provisto por los proveedores, con monitoreo continuo basado en SBOM?

Criticidad: Baja · Obligatoria en todos los niveles de criticidad (Baja, Media, Alta).

Justificación

Aun con prácticas sólidas del proveedor, la entidad es responsable de lo que se ejecuta en su propio entorno. CISA SCRM §4.14 y §4.22 piden a la entidad mantener una identificación y gestión documentadas de vulnerabilidades, incluido el escaneo del software provisto por los proveedores antes de la aceptación y de forma continua después.

Combinar este programa con el SBOM (S-06) permite a la entidad determinar, en cuestión de horas tras una nueva divulgación, si algún producto desplegado está afectado; la imposibilidad de hacerlo fue uno de los principales problemas durante Log4Shell.

Ejemplos e información adicional

Evidencia: una política de gestión de vulnerabilidades, un conjunto de herramientas (ingesta de fuentes de CVE, monitoreo de SBOM como Dependency-Track, integración del escáner con el inventario de activos), criterios de priorización (criticidad del activo, explotabilidad, exposición) y una métrica de ciclo cerrado del tiempo de mitigación por severidad.

Mapeo

Marco	Referencia / cláusula
Buenas Prácticas de ENISA (2023)	Área 3.4 — Gestión de parches; monitoreo de vulnerabilidades
Plantilla SCRM de CISA	P. 4.14, 4.22 — Gestión interna de vulnerabilidades; escaneo de vulnerabilidades antes de la aceptación
CIS Controls v8	Control 7 — Gestión Continua de Vulnerabilidades
NIST SP 800-40 Rev. 4	Guía de Gestión Empresarial de Parches

V-07 ¿Prueba la entidad los parches antes del despliegue y mantiene procedimientos de reversión / marcha atrás?

Criticidad: Media · Obligatoria en las contrataciones de criticidad Media y Alta.

Justificación

Los parches ocasionalmente provocan regresiones funcionales, rompen integraciones o — rara vez — introducen nuevas vulnerabilidades. Un ciclo de prueba previa al despliegue y un procedimiento de reversión probado son necesarios para cualquier servicio cuya indisponibilidad tenga un impacto relevante.

Las Buenas Prácticas de ENISA §3.4 incluyen específicamente la "verificación y prueba de parches" y los "procedimientos de reversión y procesos efectivos de respaldo y restauración" en la línea base de gestión de parches.

Ejemplos e información adicional

Probar los parches en un entorno de preproducción (o mediante despliegue canario) antes del despliegue amplio; documentar el procedimiento de reversión para cada servicio crítico; combinar con O-06 (respaldos independientes) e I-04 (pruebas de restauración) para que la reversión sea realista cuando se necesite.

Mapeo

Marco	Referencia / cláusula
Buenas Prácticas de ENISA (2023)	Área 3.4 — Verificación de parches, pruebas, reversión, respaldo y restauración
NIST SP 800-40 Rev. 4	Guía de Gestión Empresarial de Parches
ISO/IEC 27031	Preparación de las TIC para la continuidad del negocio

V-08 ¿Participa la entidad en la divulgación coordinada de vulnerabilidades (CVD) y en arreglos de intercambio de información (CSIRT, MISP, ISAC sectoriales)?

Criticidad: Alta · Obligatoria solo en las contrataciones de criticidad Alta.

Justificación

La madurez en la gestión de vulnerabilidades a nivel regional requiere una divulgación coordinada en lugar de intercambios bilaterales puntuales. NIS2 introduce un régimen de divulgación coordinada de vulnerabilidades con los CSIRT nacionales; las BP de ENISA §3.3 exigen el intercambio de información como parte de la gestión de las relaciones con los proveedores; la comunidad de práctica LAC4 provee el foro para la región.

Ejemplos e información adicional

Mecanismos operativos: integrarse al esquema de CVD del CSIRT nacional; suscribirse a las fuentes de los ISAC pertinentes (p. ej., financiero, energía, salud) y a una instancia de MISP; asegurar que las VDP de los proveedores (S-09) mencionen al CSIRT nacional como una de las vías de divulgación; compartir, con carácter confidencial, los indicadores de compromiso observados a través de los productos de los proveedores.

Mapeo

Marco	Referencia / cláusula
Directiva NIS2	Art. 12 — Base de datos de divulgación coordinada de vulnerabilidades

Marco	Referencia / cláusula
Buenas Prácticas de ENISA (2023)	Área 3.3 — Intercambio de información
ISO/IEC 29147	Divulgación coordinada de vulnerabilidades
Marcos CSIRT / PSIRT de FIRST.org	Patrones de coordinación

10.5 Gestión de incidentes

Los incidentes que involucran a proveedores ocurren — a veces a partir de una vulnerabilidad, a veces por un vector de ataque diferente. El objetivo de esta sección es asegurar que la entidad no se vea sorprendida cuando ocurra un incidente en un proveedor o a través de él — que el proveedor notifique a tiempo, que las responsabilidades estén claras, que la respuesta conjunta esté ensayada y que se preserve la continuidad.

I-01 ¿Están predeterminados los canales de comunicación de incidentes con el tercero, incluidas alternativas fuera de banda?

Criticidad: **Media** · Obligatoria en las contrataciones de criticidad Media y Alta.

Justificación

En un incidente de seguridad, la comunicación rápida y confiable entre ambas partes es fundamental para resolverlo. Los canales y contactos deben predeterminarse, ya que la infraestructura general de TI puede no estar disponible durante un incidente.

Ejemplos e información adicional

Acordar de antemano canales primarios y secundarios (con al menos una alternativa fuera de banda — p. ej., telefónica o basada en Signal — por si el correo se ve afectado); contactos designados de cada lado, con suplentes; cadencia de los reportes de situación; expectativas de retención legal y preservación de evidencia. Documentar fuera de los sistemas habituales de TI (copia impresa, más una entrada en la wiki).

Mapeo

Marco	Referencia / cláusula
ISO/IEC 27035	Comunicación de respuesta a incidentes
Buenas Prácticas de ENISA (2023)	Área 3.3 — Gestión de incidentes
Marco de servicios PSIRT de FIRST.org	Coordinación con las partes aguas abajo

I-02 ¿Está determinado un tiempo máximo tolerable de falla (RTO) para el servicio o producto adquirido?

Criticidad: **Media** · Obligatoria en las contrataciones de criticidad Media y Alta.

Justificación

Los servicios digitales pueden fallar por diversas razones. Si las operaciones del negocio dependen del servicio, la entidad necesita evaluar cuánto tiempo puede estar

indisponible el servicio antes de que el impacto en las operaciones se vuelva insostenible.

Ejemplos e información adicional

El RTO depende del impacto financiero, la pérdida de reputación, los efectos físicos en entornos de OT y el SLA. Una vez definido, el RTO orienta el diseño de los respaldos, los tiempos del plan de salida y los arreglos de continuidad.

Mapeo

Marco	Referencia / cláusula
ISO/IEC 22301	Sistemas de gestión de la continuidad del negocio
DORA — Reg. (UE) 2024/1774	Reporte de incidentes mayores / RTO
Buenas Prácticas de ENISA (2023)	Área 3.3 — Continuidad del negocio

I-03 ¿Está determinado cómo continúan las operaciones sin el uso del servicio o producto adquirido (plan de continuidad del negocio)?

Criticidad: Media · Obligatoria en las contrataciones de criticidad Media y Alta.

Justificación

Si un servicio o producto falla durante un período prolongado, las operaciones del negocio pueden volverse imposibles y la entidad queda en riesgo. Un plan de continuidad del negocio (BCP) previene daños significativos.

La insolvencia, el ransomware o una disrupción geopolítica — cualquiera de ellos puede dejar al proveedor indisponible por un período extendido. La P. 8.3 de CISA SCRM convierte un BCP formal en una obligación independiente del proveedor.

Ejemplos e información adicional

El BCP debería describir cómo el servicio puede reemplazarse al menos temporalmente — un servicio alternativo con capacidades similares, el manejo manual de los procesos, un proveedor secundario o una alternativa interna. Incluir la extracción de datos en el BCP.

Panorama de Amenazas de ENISA — caso ilustrativo: Kaseya (julio de 2021) — los clientes de proveedores de servicios gestionados se vieron afectados durante días; las entidades con una alternativa manual para el flujo de trabajo afectado sufrieron menos impacto.

Mapeo

Marco	Referencia / cláusula
Directiva NIS2	Art. 21(2)(c) — continuidad del negocio
DORA — Reg. (UE) 2022/2554	Resiliencia operativa y estrategias de salida

Marco	Referencia / cláusula
Buenas Prácticas de ENISA (2023)	Área 3.3 — Continuidad del negocio
ISO/IEC 22301	Sistemas de gestión de la continuidad del negocio
Plantilla SCRM de CISA	P. 8.3, 8.6, 8.7 — BCP / diversidad de proveedores

I-04 ¿Se prueban las operaciones de restauración de respaldos a intervalos regulares?

Criticidad: Media · Obligatoria en las contrataciones de criticidad Media y Alta.

Justificación

Crear respaldos con regularidad es fundamental, pero muchas organizaciones no prueban si un respaldo realmente puede restaurarse. El procedimiento de restauración debería probarse periódicamente en un entorno limpio.

Ejemplos e información adicional

Probar la restauración al menos una vez al año para todos los servicios críticos. Documentar el tiempo de restauración, la integridad de los datos y cualquier desviación. La P. 4.26 de CISA SCRM incluye la prueba de los medios de respaldo como parte del proceso de recuperación del proveedor.

Mapeo

Marco	Referencia / cláusula
ISO/IEC 27031	Preparación de las TIC para la continuidad del negocio
CIS Controls v8	Control 11 — Recuperación de Datos
Plantilla SCRM de CISA	P. 4.26 — Frecuencia de las pruebas de los medios de respaldo

I-05 ¿Se preparan guías de respuesta conjuntas para la gestión de incidentes con cada proveedor crítico?

Criticidad: Alta · Obligatoria solo en las contrataciones de criticidad Alta.

Justificación

Los planes genéricos de incidentes rara vez sobreviven al contacto con un incidente de cadena de suministro. Una guía de respuesta adaptada a cada proveedor crítico — con contactos, rutas de escalamiento y decisiones clave — ahorra horas preciosas durante la respuesta.

Ejemplos e información adicional

Mantener una guía de respuesta de una página para cada proveedor crítico que cubra: los contactos en el proveedor (operativos y ejecutivos); las acciones esperadas del proveedor; las acciones de la entidad (p. ej., revocar la conectividad, cambiar al respaldo); la comunicación a las partes interesadas internas y a los reguladores. Probar la guía al menos una vez al año con el proveedor.

Mapeo

Marco	Referencia / cláusula
Directiva NIS2	Art. 21(2)(b) — gestión de incidentes

Marco	Referencia / cláusula
Buenas Prácticas de ENISA (2023)	Área 3.3 — Respuesta conjunta a incidentes
ISO/IEC 27035	Gestión de incidentes
DORA — Reg. (UE) 2024/1774	Pruebas conjuntas

I-06 ¿Está definida la notificación contractual de incidentes (con plazos compatibles con NIS2)?

Criticidad: Baja · Obligatoria en todos los niveles de criticidad (Baja, Media, Alta).

Justificación

Cuando la propia entidad es una entidad esencial o importante bajo NIS2 — o bajo un equivalente nacional — tiene plazos de notificación estrictos (alerta temprana a las 24 horas, notificación a las 72 horas, informe final al mes). Los proveedores deben notificar a la entidad a tiempo para que esta pueda cumplir.

Ejemplos e información adicional

El contrato debería exigir al proveedor notificar a la entidad sin demora indebida y, en todo caso, dentro de un número definido de horas tras la detección, y proporcionar actualizaciones a medida que avance la respuesta. El formato de notificación debería acordarse por adelantado.

Mapeo

Marco	Referencia / cláusula
Directiva NIS2	Art. 23 — obligaciones de reporte
Buenas Prácticas de ENISA (2023)	Área 3.3 — Notificación
DORA — Reg. (UE) 2024/1774	Reporte de incidentes mayores

I-07 ¿Forman parte del contrato las obligaciones de reporte de incidentes y las penalidades contractuales / créditos de servicio?

Criticidad: Media · Obligatoria en las contrataciones de criticidad Media y Alta.

Justificación

Los incentivos importan. Un proveedor que no asume ninguna consecuencia contractual por una notificación tardía o por incidentes causados por su propia negligencia tiene incentivos más débiles para invertir en prevención.

Ejemplos e información adicional

Los créditos de servicio o las penalidades contractuales deberían calibrarse según la criticidad del servicio. No sustituyen la indemnización por daños. El contrato también debería definir cuándo un incidente es lo suficientemente grave como para activar un derecho contractual de terminación.

Mapeo

Marco	Referencia / cláusula
DORA — Reg. (UE) 2024/1773	Derechos de terminación y remedios
ISO/IEC 27036-2	Remedios contractuales
Buenas Prácticas de ENISA (2023)	Área 3.3 — Remedios

I-08 ¿Existe una revisión posterior al incidente, conjunta o coordinada con el tercero, con acciones correctivas designadas y plazos?

Criticidad: Media · Obligatoria en las contrataciones de criticidad Media y Alta.

Justificación

Los ejercicios de lecciones aprendidas que incluyen al proveedor son mucho más efectivos que las revisiones solo internas. El proveedor es a menudo la única parte que puede explicar la causa raíz y la trayectoria de la respuesta.

Ejemplos e información adicional

Dentro de un período definido tras el cierre de un incidente mayor, realizar una revisión conjunta que cubra: la cronología, la causa raíz, lo que funcionó, lo que no, y acciones correctivas concretas de cada lado, con responsables y plazos. Dar seguimiento a las acciones correctivas hasta su cierre.

Mapeo

Marco	Referencia / cláusula
ISO/IEC 27035-2	Lecciones aprendidas
Buenas Prácticas de ENISA (2023)	Área 3.3 — Mejora continua
Directiva NIS2	Art. 23 — informe final
Plantilla SCRM de CISA	P. 3.17 — Causa raíz de las vulnerabilidades

10.6 Desmantelamiento / Fin de uso

El fin del contrato es un momento de alto riesgo. La entidad debe poder llevarse sus datos, no dejar accesos residuales, impedir que el proveedor retenga o reutilice los datos de la entidad y mantener la confidencialidad de la información compartida durante la relación.

D-01 ¿Se prepara con antelación un plan de desmantelamiento, que incluya los tiempos, el período de transición y las responsabilidades designadas?

Criticidad: Media · Obligatoria en las contrataciones de criticidad Media y Alta.

Justificación

Cuando un producto o servicio se retira de uso sin considerar todos los efectos, las operaciones del negocio pueden verse afectadas. Un plan detallado para la transición evita sorpresas.

Ejemplos e información adicional

El plan de desmantelamiento debería incluir, como mínimo: cuándo se terminará el contrato; cuándo el producto o servicio dejará de estar disponible para uso productivo; cuándo se informará a los usuarios; cuánto durará el período de transición; quién es responsable de cada paso; y qué datos deben exportarse.

Mapeo

Marco	Referencia / cláusula
Buenas Prácticas de ENISA (2023)	Área 3.3 — Gestionar a los proveedores a lo largo de todo el ciclo de vida
DORA — Reg. (UE) 2022/2554	Estrategias de salida
ISO/IEC 27036-2	Fin de la relación

D-02 ¿Participan todas las partes interesadas pertinentes en el desmantelamiento?

Criticidad: Media · Obligatoria en las contrataciones de criticidad Media y Alta.

Justificación

Al igual que la implementación de un nuevo servicio, el desmantelamiento puede afectar a diversas partes. Pueden perderse perspectivas valiosas si no se consulta a ciertas partes interesadas. Todas las partes interesadas afectadas deberían participar en la fase de desmantelamiento.

Ejemplos e información adicional

Las partes interesadas dependen del contexto — en general aplica la misma lista que para la contratación (P-05).

- Personal de TI y de operaciones
- Oficiales de ciberseguridad / CISO
- Empleados (o sus representantes)
- Clientes y ciudadanos (cuando corresponda)
- Proveedores o suplidores existentes que dependan del sistema
- Autoridades
- Entidades asociadas
- Asesores legales

Mapeo

Marco	Referencia / cláusula
ISO/IEC 27036-2	Fin de la relación
Buenas Prácticas de ENISA (2023)	Área 3.3 — Ciclo de vida

D-03 ¿Se exportan todos los datos que deban archivarse o utilizarse en el futuro antes de perder el acceso?

Criticidad: Baja · Obligatoria en todos los niveles de criticidad (Baja, Media, Alta).

Justificación

Después de que un servicio deja de usarse, los datos procesados y almacenados por este suelen volverse inaccesibles. Los datos deben exportarse antes de perder el acceso. La importación a un nuevo servicio puede tomar tiempo, y ese tiempo debe planificarse.

Ejemplos e información adicional

Utilizar el formato de exportación acordado bajo S-10 (portabilidad de datos). Validar la completitud y la integridad de la exportación. Documentar la cadena de custodia del proveedor a la entidad (o al proveedor sucesor).

Mapeo

Marco	Referencia / cláusula
Evaluación de Riesgos de Computación en la Nube de ENISA	Dependencia (lock-in) / salida
Ley de Datos de la UE — Reg. (UE) 2023/2854	Obligaciones de cambio de proveedor
DORA — Reg. (UE) 2022/2554	Estrategias de salida
ISO/IEC 27036-2	Fin de la relación

D-04 ¿Se eliminan todos los datos confidenciales de los servidores de terceros, con una atestación verificable?

Criticidad: Baja · Obligatoria en todos los niveles de criticidad (Baja, Media, Alta).

Justificación

Si un servicio procesa y almacena datos en servidores de terceros, esa información puede seguir en los sistemas de terceros después de terminado el contrato. El proceso de desmantelamiento debería incluir pasos verificables para eliminar todos los datos en los sistemas de terceros, incluidos los respaldos.

Los datos a eliminar también pueden estar definidos en requisitos externos, contratos y leyes.

Ejemplos e información adicional

Exigir al proveedor una atestación escrita que especifique los sistemas, el método (borrado criptográfico, eliminación segura, destrucción física) y la fecha. La entidad debería conservar el derecho a verificar o a encargar una verificación independiente. Abordar explícitamente los respaldos, incluido el plazo para que los datos salgan de la cadena de respaldos.

Mapeo

Marco	Referencia / cláusula
NIST SP 800-88	Directrices para la sanitización de medios
ISO/IEC 27036-2	Fin de la relación — devolución / destrucción de datos
ISO/IEC 27040	Seguridad del almacenamiento

D-05 ¿Se desactivan todas las instalaciones del producto y todas las cuentas del servicio al finalizar el contrato?

Criticidad: Baja · Obligatoria en todos los niveles de criticidad (Baja, Media, Alta).

Justificación

Después de que termina el contrato del producto o servicio, las instalaciones suelen dejar de recibir actualizaciones de seguridad y los acuerdos de licencia a menudo prohíben el uso continuado. Todas las cuentas e instalaciones deberían ser deshabilitadas por los administradores.

Ejemplos e información adicional

Mantener una lista de verificación que vincule las cuentas y las instalaciones con el contrato. Confirmar la desactivación y conservar los registros.

Mapeo

Marco	Referencia / cláusula
ISO/IEC 27036-2	Fin de la relación
Buenas Prácticas de ENISA (2023)	Área 3.3 — Ciclo de vida
Plantilla SCRM de CISA	P. 6.6 — Desvinculación

D-06 ¿Se mantienen las obligaciones de confidencialidad / NDA más allá del fin del contrato?

Criticidad: Baja · Obligatoria en todos los niveles de criticidad (Baja, Media, Alta).

Justificación

La información compartida durante el contrato — arquitectura, vulnerabilidades, historial de incidentes, procesos de negocio — sigue siendo sensible mucho después de que el contrato termina. Las obligaciones de confidencialidad de duración estándar (típicamente de 3 a 5 años posteriores al contrato) deberían acordarse a la firma.

Ejemplos e información adicional

El contrato debería especificar la duración de las obligaciones de confidencialidad después de la terminación, listar las categorías de información cubiertas y definir las consecuencias del incumplimiento.

Mapeo

Marco	Referencia / cláusula
ISO/IEC 27036-2	Confidencialidad y protección de la información
ISO/IEC 27001:2022	Anexo A.6.6 — Acuerdos de confidencialidad o no divulgación

D-07 ¿Se aborda la sanitización / disposición del hardware al final de su vida útil (cuando se adquiere hardware)?

Criticidad: Alta · Obligatoria solo en las contrataciones de criticidad Alta.

Justificación

El hardware que sale del control de la entidad puede contener datos residuales. El proveedor del hardware (o un proveedor de disposición final) debería sanitizar los medios conforme a estándares reconocidos antes de su disposición, y la cadena de custodia debería documentarse.

Ejemplos e información adicional

Exigir evidencia de sanitización conforme a NIST SP 800-88 o equivalente. Para el hardware al final de su vida útil enviado a un proveedor de disposición final, exigir un documento de cadena de custodia y un certificado de destrucción. Cuando el hardware haya sido arrendado, asegurar que el arrendador no pueda devolverlo al mercado sin sanitización.

Mapeo

Marco	Referencia / cláusula
NIST SP 800-88	Directrices para la sanitización de medios
ISO/IEC 27040	Seguridad del almacenamiento
Buenas Prácticas de ENISA (2023)	Área 3.5 — Ciclo de vida del hardware
Plantilla SCRM de CISA	P. 7.11 — Reutilización / reciclaje

11. Definiciones

A lo largo de este documento se utilizan los siguientes términos.

Entidad: Usuario de esta directriz. La organización que adquiere servicios o productos de terceros y es responsable de gestionar el riesgo de la cadena de suministro.

Proveedor / tercero: Cualquier organización que provea un servicio o producto utilizado por la entidad, incluidos los proveedores de software, los fabricantes de hardware, los proveedores de nube, los proveedores de servicios gestionados (MSP), los proveedores de servicios de seguridad gestionados (MSSP) y las consultoras.

Subencargado / cuarta parte: Una organización contratada por un proveedor de la entidad para entregar parte del servicio o producto contratado. Desde la perspectiva de la entidad, son proveedores indirectos.

Ciclo de vida de la contratación: La secuencia completa desde la identificación de necesidades, el análisis de mercado, la precalificación de proveedores, la licitación, la contratación, la entrega, la operación, el monitoreo y el desmantelamiento.

Nivel de criticidad de la contratación: Clasificación Baja / Media / Alta asignada a una contratación según la sensibilidad de los datos procesados, el impacto de la indisponibilidad y el régimen regulatorio. Determina qué preguntas del Cuestionario para Proveedores son obligatorias.

Servicio o producto crítico: Un servicio o producto cuya falla o vulneración tendría un impacto significativo en la misión de la entidad o en el público.

SBOM: Lista de Materiales de Software (Software Bill of Materials): un inventario formal y legible por máquina de los componentes que conforman un producto de software (CycloneDX o SPDX).

VDP: Política de Divulgación de Vulnerabilidades (Vulnerability Disclosure Policy): una política pública que describe cómo los investigadores pueden reportar vulnerabilidades al proveedor de manera responsable y cómo el proveedor las gestiona.

PSIRT: Equipo de Respuesta a Incidentes de Seguridad de Productos (Product Security Incident Response Team): la función del proveedor responsable de recibir, clasificar, priorizar, remediar y comunicar las vulnerabilidades de los productos.

CVD: Divulgación Coordinada de Vulnerabilidades (Coordinated Vulnerability Disclosure): un proceso mediante el cual una vulnerabilidad se divulga a múltiples partes de manera coordinada — típicamente el proveedor, un CSIRT nacional y, en última instancia, el público.

SDL / SSDF: Ciclo de Vida de Desarrollo Seguro / Marco de Desarrollo Seguro de Software: un proceso estructurado mediante el cual las actividades de seguridad se integran en cada etapa del desarrollo de software. NIST SP 800-218 (SSDF) es una referencia destacada.

SGSI: Sistema de Gestión de Seguridad de la Información: un marco sistemático para gestionar los riesgos de seguridad de la información (p. ej., ISO/IEC 27001).

Ataque a la cadena de suministro: Según ENISA: una combinación de al menos dos ataques — uno contra un proveedor y otro utilizado para atacar al cliente a través de ese proveedor.

NIS2: Directiva (UE) 2022/2555 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión.

CRA: Reglamento (UE) 2024/2847, el Reglamento de Ciberresiliencia de la UE, sobre requisitos horizontales de ciberseguridad para los productos con elementos digitales.

DORA: Reglamento (UE) 2022/2554 sobre la resiliencia operativa digital del sector financiero.

ENISA: Agencia de la Unión Europea para la Ciberseguridad.

12. Anexo A — Estándares para una Cadena de Suministro Cibersegura

Este anexo consolida los estándares que los proveedores deberían cumplir a lo largo del ciclo de vida. Cada estándar se resume, y las entidades pueden referenciarlos directamente en los documentos de licitación o en las cláusulas contractuales.

A.1 Lista de Materiales de Software (SBOM)

- Requerido: toda contratación de software / servicios digitales.
- Formato: legible por máquina; se aceptan CycloneDX o SPDX; profundidad: al menos un nivel más allá del código propio.
- Cadencia: en la aceptación y en cada versión mayor.
- Referencia: CRA de la UE, Anexo I, Parte II; Elementos Mínimos de SBOM de NTIA / CISA.

A.2 Políticas de Divulgación de Vulnerabilidades (VDP)

- Requerido: todo proveedor de productos / servicios digitales.
- Contenido: punto de contacto público, plazo de acuse de recibo, proceso de triaje y divulgación.
- Referencia: ISO/IEC 29147, ISO/IEC 30111, CRA de la UE Arts. 13-14.

A.3 Certificación de seguridad y niveles de aseguramiento

- Mapeo por nivel de riesgo: riesgo bajo → ISO/IEC 27001 o equivalente; medio → ISO/IEC 27001 + conformidad a nivel de producto (CRA Anexo I); alto → EUCC / EUCS / esquemas sectoriales.
- Validación: certificado, alcance, vencimiento, organismo acreditador, informe de auditoría reciente.
- Referencia: Ley de Ciberseguridad de la UE (Reg. (UE) 2019/881); EUCC (Reg. (UE) 2024/482); EUCS (en adopción).

A.4 Ciclo de Vida de Desarrollo Seguro (SDL) e integridad del entorno de compilación

- Estándares documentados de codificación segura.
- Modelado de amenazas para toda versión que contenga cambios relevantes.
- Revisión por pares obligatoria y pruebas de seguridad (SAST, DAST, escaneo de dependencias, fuzzing).
- Firma de código de las versiones; compilaciones reproducibles; acceso restringido a la infraestructura de compilación; auditoría del entorno de compilación.
- Alineación opcional con SLSA de Google (Supply chain Levels for Software Artifacts).

- Capacitación en seguridad de los desarrolladores; capacitación periódica.
- Referencia: NIST SSDF (SP 800-218), ISO/IEC 27034, CRA de la UE Anexo I, Plantilla SCRM de CISA P. 3.6, 3.7, 3.10, 3.13.

A.5 Gestión de vulnerabilidades — proveedor y entidad

- Lado del proveedor: función equivalente a un PSIRT; análisis formal de vulnerabilidades y debilidades en cada versión; análisis de causa raíz cuyas lecciones se incorporan al SDL; política de mantenimiento por niveles de riesgo basada en CVSS; cadencia de notificación proactiva a los clientes.
- Lado de la entidad: programa interno de gestión de vulnerabilidades; monitoreo continuo del SBOM frente a las nuevas divulgaciones; procedimientos de prueba de parches y reversión; participación en los arreglos del CSIRT nacional y de CVD.
- Referencia: Buenas Prácticas de ENISA, Área 3.4; CISA SCRM §3.14-3.17 y §4.14-4.23; ISO/IEC 29147 / 30111; NIST SP 800-40 Rev. 4; NIS2 Art. 12.

A.6 Integridad del hardware (cuando se adquiere hardware)

- Abastecimiento exclusivo de OEM o revendedores autorizados para los componentes clave.
- Embalaje que evidencie cualquier apertura o manipulación, y documentación de cadena de custodia en tránsito.
- Procesos de prevención de falsificaciones en el proveedor.
- Sanitización conforme a NIST SP 800-88 al final de la vida útil.
- Referencia: Plantilla SCRM de CISA P. 2.6, 2.7, 5.8-5.10, 7.11.

A.7 Reporte de incidentes y penalidades contractuales

- Plazo de notificación alineado con las obligaciones NIS2 de la entidad.
- Canales de comunicación acordados de antemano (primario y fuera de banda).
- Créditos de servicio / penalidades calibrados según la criticidad.
- Derecho de terminación por incumplimientos reiterados o graves.
- Referencia: NIS2 Art. 23, DORA Reg. (UE) 2024/1774.

13. Anexo B — Guía práctica: evaluación mínima de riesgos de proveedores

Este anexo ofrece una metodología mínima de seis pasos que los equipos de compras y de seguridad pueden utilizar sin experiencia previa en marcos formales de gestión de riesgos. No sustituye a ISO/IEC 27005 ni a NIST SP 800-30 para las entidades que ya operan alguno de ellos — es un punto de partida.

B.1 Paso 1 — Caracterizar la contratación

¿Qué servicio o producto se está adquiriendo? ¿Qué datos procesa? ¿Cuál es la clasificación más alta? ¿Cuál es el tiempo máximo tolerable de indisponibilidad? ¿La pérdida máxima tolerable de datos? ¿De qué otros sistemas depende? ¿Qué procesos / servicios de la entidad dependen de él? Utilizar las respuestas para asignar un nivel de criticidad de la contratación (Baja / Media / Alta) que determinará qué preguntas son obligatorias.

B.2 Paso 2 — Identificar al proveedor y la profundidad de la cadena de suministro

¿Quién es la parte contratante? ¿Quién es la parte operadora? ¿Dónde tiene su sede el proveedor? ¿Desde dónde opera el servicio? ¿Qué subencargados participan? ¿Alguno de ellos es crítico para el servicio?

B.3 Paso 3 — Identificar los escenarios de amenaza (utilizar la taxonomía de ENISA)

El Panorama de Amenazas de ENISA (2021) clasifica los ataques por: técnica de ataque al proveedor, activo del proveedor atacado, técnica de ataque al cliente, activo del cliente atacado. Utilizar esta taxonomía para caracterizar escenarios específicos de la contratación.

B.4 Paso 4 — Estimar la probabilidad y el impacto

Una matriz de 3x3 (Baja / Media / Alta en cada eje) es suficiente a este nivel. Para cada escenario, documentar la probabilidad asumida y el impacto asumido en una nota de una línea que explique el razonamiento.

B.5 Paso 5 — Identificar y escalonar los controles

Mapear las recomendaciones aplicables de este documento a los escenarios. Para cada escenario, anotar qué recomendaciones lo mitigan y a qué nivel (prevenir / detectar / responder / recuperar).

B.6 Paso 6 — Decidir y documentar

Para cada riesgo residual, documentar una de las siguientes opciones: aceptar (con un responsable del riesgo designado), transferir (p. ej., remedios contractuales, seguros), mitigar (con acciones y plazos designados) o evitar (no adquirir el servicio de este proveedor). La decisión y el razonamiento subyacente deberían ser visibles para el grupo de gobernanza de contrataciones.

B.7 Ejemplos de amenazas del Panorama de Amenazas de ENISA

- SolarWinds Orion (diciembre de 2020) — código del proveedor modificado durante el proceso de compilación; alrededor de 18,000 clientes recibieron la actualización maliciosa.
- Mimecast (enero de 2021) — un certificado comprometido del proveedor se utilizó para autenticarse en los inquilinos (tenants) de Microsoft 365 de los clientes.
- Codecov (abril de 2021) — credenciales robadas de una imagen de Docker se utilizaron para modificar el script bash de cara a los clientes.
- Verkada (marzo de 2021) — credenciales encontradas en línea (OSINT) dieron a los atacantes acceso a 150,000 cámaras de clientes.
- Kaseya VSA (julio de 2021) — un zero-day utilizado para distribuir ransomware a través del canal de actualización del proveedor.

B.8 Ejemplos de mitigaciones de estas directrices

- S-08 (SDL) y S-18 (integridad del entorno de compilación) mitigan el patrón de SolarWinds / Codecov.
- S-13 (verificación del personal) y O-09 (cuentas nominativas, MFA, JIT para el personal del proveedor) mitigan el patrón de Verkada.
- V-04 (política de mantenimiento basada en CVSS) + V-06 (gestión de vulnerabilidades del lado de la entidad con monitoreo de SBOM) + O-11 (SLA de parches) mitigan la vulnerabilidad en cascada al estilo Log4Shell.
- S-14 (control de subencargados) y S-15 (cambio de control / ubicación) mitigan el patrón de cambio de subencargados.
- S-10 (portabilidad de datos) y D-01 a D-04 (desmantelamiento) mitigan los patrones de dependencia del proveedor y de pérdida de datos.

14. Referencias

- Directiva (UE) 2022/2555 (NIS2)
- Reglamento (UE) 2024/2847 (Reglamento de Ciberresiliencia)
- Reglamento (UE) 2019/881 (Ley de Ciberseguridad)
- Reglamento (UE) 2022/2554 (DORA)
- Reglamento Delegado (UE) 2024/1773 de la Comisión (RTS sobre política de terceros de TIC)
- Reglamento Delegado (UE) 2024/1774 de la Comisión (RTS sobre gestión de riesgos de TIC)
- Reglamento Delegado (UE) 2025/532 de la Comisión (RTS sobre subcontratación)
- Reglamento de Ejecución (UE) 2024/482 de la Comisión (esquema EUCC)
- Reglamento de Ejecución (UE) 2024/2690 de la Comisión — y Guía de Implementación Técnica de ENISA
- Reglamento (UE) 2023/2854 (Ley de Datos)
- ENISA — Buenas Prácticas para la Ciberseguridad de la Cadena de Suministro (junio de 2023)
- ENISA — Panorama de Amenazas sobre Ataques a la Cadena de Suministro (julio de 2021)
- ENISA — Evaluación de Riesgos de Computación en la Nube
- Caja de Herramientas de la UE para la Seguridad de la Cadena de Suministro de TIC
- ISO/IEC 27001:2022 — Sistemas de gestión de seguridad de la información
- ISO/IEC 27036 — Seguridad de la información en las relaciones con proveedores (varias partes)
- ISO/IEC 27005 — Gestión de riesgos de seguridad de la información
- ISO/IEC 27035 — Gestión de incidentes (varias partes)
- ISO/IEC 27040 — Seguridad del almacenamiento
- ISO/IEC 27034 — Seguridad de las aplicaciones
- ISO/IEC 22301 — Sistemas de gestión de la continuidad del negocio
- ISO/IEC 19086 — Marco de SLA para la nube
- ISO/IEC 19941 / 22123 — Interoperabilidad y portabilidad en la nube
- ISO/IEC 29147 — Divulgación de vulnerabilidades
- ISO/IEC 30111 — Procesos de tratamiento de vulnerabilidades
- NIST SP 800-161 Rev.1 — Prácticas de Gestión de Riesgos de la Cadena de Suministro de Ciberseguridad
- NIST SP 800-218 — Marco de Desarrollo Seguro de Software (SSDF)
- NIST SP 800-30 — Guía para Realizar Evaluaciones de Riesgo

- NIST SP 800-40 Rev. 4 — Guía de Gestión Empresarial de Parches
- NIST SP 800-88 — Directrices para la Sanitización de Medios
- NIST SP 800-207 — Arquitectura de Confianza Cero (Zero Trust)
- CIS Controls v8 y CIS Benchmarks
- CISA / Grupo de Trabajo ICT SCRM — Plantilla SCRM para Proveedores (abril de 2021)
- CISA / NTIA — Elementos Mínimos de SBOM
- FIRST.org — Marco de Servicios PSIRT
- FIRST.org — CVSS (Sistema Común de Calificación de Vulnerabilidades)
- Google — SLSA (Supply chain Levels for Software Artifacts)
- MITRE — ATT&CK® y D3FEND
- Banco Interamericano de Desarrollo / OEA — Reporte de Ciberseguridad 2025 (ALC)
- Índice Nacional de Ciberseguridad (NCSI) — e-Governance Academy