SECURE
Cyber Resilience for SMEs

Requisitos esenciales de ciberseguridad de la Cyber Resilience Act (CRA): Anexo I, Parte I

20/10/2025

Funded by the European Union

Declaración de financiación de la UE: Financiado por la Unión Europea con el número GA 101190325. Las opiniones y puntos de vista expresados son, sin embargo, exclusivamente del autor o autores y no reflejan necesariamente los de la Unión Europea ni los del Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad. Ni la Unión Europea ni la autoridad que concede la subvención se hacen responsables de ellas.

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Descargo de responsabilidad del ECCC: El proyecto cuenta con el apoyo del Centro Europeo de Competencia en Ciberseguridad y sus miembros.

EXENCIÓN DE RESPONSABILIDAD

Este documento forma parte del entregable D4.1 «Directrices y materiales para el cumplimiento de la CRA por parte de las pymes» del proyecto SECURE

Este documento ha sido traducido al español utilizando como apoyo un sistema de traducción automática, por lo que podría contener inexactitudes o errores.

Autor principal: *Centro de Ciberseguridad de Bélgica (CCB)*

Segundo autor: *Autoritatea Pentru Digitalizarea Romaniei-NCC-RO (ADR-NCC-RO)*

Índice

Lista de tablas y figuras

Abreviaturas

API: Interfaz de programación de aplicaciones

APT: Amenazas persistentes avanzadas

BSIMM: Modelo de madurez para la seguridad en el desarrollo de software

CI/CD: Integración continua y entrega/implementación continua

CRA: Ley de Resiliencia Cibernética (Cyber Resilience Act)

CVD: Divulgación coordinada de vulnerabilidades (Coordinated Vulnerability Disclosure)

CVE: Vulnerabilidades y exposiciones comunes (Common Vulnerabilities and Exposures)

CVSS: Sistema común de puntuación de vulnerabilidades

DAST: Pruebas dinámicas de seguridad de aplicaciones

DoS: Denegación de servicio

DREAD: Daño, reproducibilidad, explotabilidad, usuarios afectados y detectabilidad

ENISA: Agencia de la Unión Europea para la Ciberseguridad

EOL: Fin de vida útil

EPSS: Sistema de puntuación de predicción de vulnerabilidades

ETSI: Instituto Europeo de Normas Técnicas

UE – Unión Europea

FIRST VCMM: Modelo de madurez de coordinación de vulnerabilidades de FIRST

RGPD – Reglamento General de Protección de Datos

HTTPS/TLS: Protocolo de hipertexto seguro/Seguridad de la capa de transporte

ICS – Sistema de control industrial

IEC – Comisión Electrotécnica Internacional

IoT: Internet de las cosas

IPSec: Protocolo de seguridad de Internet

ISO: Organización Internacional de Normalización

JTAG – Grupo de Acción Conjunta de Pruebas

LINDDUN: Vinculación, identificación, no repudio, detección, divulgación de datos, desconocimiento e incumplimiento

MFA: Autenticación multifactorial

MITRE ATT&CK: Tácticas, técnicas y conocimientos comunes adversarios

MQTT – Transporte de telemetría con colas de mensajes

NIST: Instituto Nacional de Estándares y Tecnología (Estados Unidos)

NIST SSDF: Marco de desarrollo de software seguro del NIST

NTIA: Administración Nacional de Telecomunicaciones e Información (Estados Unidos)

OPENSSF VEX: Intercambio de vulnerabilidades y explotabilidad de la Fundación de Seguridad de Código Abierto

OS – Sistema operativo

OTA – A través del aire (Over-The-Air)

OWASP: Proyecto mundial abierto de seguridad de aplicaciones

OWASP ASVS – Estándar de verificación de seguridad de aplicaciones de OWASP

OWASP SAMM: Modelo de madurez de garantía de software de OWASP

PDE: Producto con elementos digitales

PSIRT – Equipo de respuesta a incidentes de seguridad de productos

SAST: Pruebas estáticas de seguridad de aplicaciones

SBOM: Lista de materiales de software

SCA: Análisis de composición de software

SIEM: Gestión de información y eventos de seguridad

PYME: Pequeña y mediana empresa

SOC: Centro de operaciones de seguridad

SQL: Lenguaje de consulta estructurado

SSDLC: Ciclo de vida seguro del desarrollo de software

SSL – Capa de sockets seguros

STRIDE: Suplantación, manipulación, repudio, divulgación de información, denegación de servicio, elevación de privilegios

TPM: Módulo de plataforma de confianza

UART: Receptor-transmisor asíncrono universal

USB: Bus serie universal

VPN: Red privada virtual

Introducción

Con el fin de cumplir con la **Ley de Resiliencia Cibernética** (CRA), Reglamento (UE) 2024/2847, dirigiéndose a los fabricantes, la CRA estipula una multitud de requisitos y obligaciones. Una de las más importantes es que se debe garantizar que el producto con elementos digitales (PDE) que se comercializa «ha sido diseñado, desarrollado y fabricado de conformidad con los requisitos esenciales de ciberseguridad establecidos en la parte I del anexo I»[1] . El anexo I consta de dos partes: la parte I se centra en los requisitos de ciberseguridad relacionados con las propiedades del producto, y la parte II examina los requisitos de gestión de vulnerabilidades. La parte I consta a su vez de dos puntos, el primero de los cuales estipula que

> *« Los productos con elementos digitales se diseñarán, desarrollarán y producirán de manera que garanticen un nivel adecuado de ciberseguridad sobre la base de los riesgos existentes. »*[2]

El punto 2 especifica los requisitos que deben cumplir sus productos.

Esta guía, elaborada en el marco **del proyecto** SECURE[3] con el objetivo de **apoyar a las pequeñas y medianas empresas (PYMEs)**, profundiza en los dos puntos de la parte I del anexo I y ofrece **sugerencias prácticas y técnicas no exhaustivas, ejemplos y enfoques para ayudar a cumplir cada requisito**. Es importante señalar que cualquier referencia a normas, herramientas y marcos existentes es de **carácter** puramente **orientativo**, con la intención de que los requisitos de la CRA sean lo más tangibles posible. Las recomendaciones formuladas se basan en las mejores prácticas reconocidas y en enfoques comunes. Tanto las herramientas a las que se hace referencia en la guía como la propia guía se actualizarán a medida que avance el desarrollo de normas específicas de la CRA y de las medidas de ejecución de la Comisión Europea a lo largo del período de adaptación de 2024 a 2027.

[1] Art. 13(1), CRA.

[2] Anexo I, parte I, apartado 1, CRA.

[3] El proyecto «Fortalecimiento de la ciberresiliencia de las pymes de la UE» (SECURE) ofrece apoyo financiero y orientación a las pymes para que cumplan con la CRA.

Requisitos esenciales de ciberseguridad de la CRA: Anexo I, Parte I

1. Enfoque de ciberseguridad basado en el riesgo

El punto 1 del anexo I, parte I, estipula que

> *« Los productos con elementos digitales se diseñarán, desarrollarán y producirán de manera que garanticen **un nivel adecuado de ciberseguridad sobre la base de los riesgos existentes.**»*[4] .

Este punto es fundamental para la CRA y se basa en el principio de «seguridad desde el diseño y por defecto». En esencia, significa que debe desarrollar un **enfoque de ciberseguridad basado en el riesgo** para su producto. Esta adaptación basada en el riesgo debe ser defendible, documentada y proporcionada. Piense en el cumplimiento de la CRA como un «recorrido trazable»:

contexto del producto → riesgo → controles → prueba

La justificación de este recorrido debe documentarse diligentemente en la documentación técnica obligatoria[5] , crucial para el cumplimiento y la auditabilidad.

En la práctica, los fabricantes deben:

1. Evaluar los riesgos de ciberseguridad asociados al PDE a lo largo de su ciclo de vida;
2. Adaptar las medidas de seguridad al nivel de riesgo (por ejemplo, un termostato inteligente frente a un sistema de control industrial);
3. Tener en cuenta los modelos de amenazas, las superficies de ataque y el impacto potencial en los usuarios y los sistemas.

Por lo tanto, un primer paso crucial para cumplir con la CRA es realizar una **evaluación de riesgos** para su PDE. En este capítulo se analiza cómo llevar a cabo dicha evaluación de riesgos, estableciendo posibles enfoques y ofreciendo sugerencias técnicas.

Antes de entrar en detalles, a continuación, se ofrece una descripción general de dos páginas **sobre la evaluación de riesgos 101** para refrescar la memoria. Los elementos vuelven a aparecer con mayor detalle en el primer capítulo de esta guía, el cual se recomienda consultar. Sin embargo, por motivos de accesibilidad, el resumen simplificado expone cómo se abordan generalmente las evaluaciones de riesgos[6] .

[4] Anexo I, parte I, apartado 1, CRA.

[5] Art. 31, CRA.

[6] Es fundamental señalar que la Comisión Europea aún no ha elaborado orientaciones oficiales sobre cómo llevar a cabo la evaluación de riesgos para la CRA en concreto. Las orientaciones que se ofrecen aquí resumen

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Evaluación de riesgos 101

A la hora de realizar una evaluación de riesgos, se pueden tener en cuenta **seis pasos**:

1) Identificación de **activos** y **amenazas** = *identificar cada activo (lo que hay que proteger) según su exposición a una amenaza (lo que podría salir mal);*
2) Evaluación de **vulnerabilidades** = *evaluar las vulnerabilidades*;
3) Consideración y evaluación de **los impactos** y **la probabilidad** = *trazar los impactos y la probabilidad de las vulnerabilidades → esto da como resultado «riesgos» específicos*;
4) **Análisis** y **aceptación** de riesgos = *identificar cada riesgo y considerar su nivel de aceptación para priorizar sus acciones;*

Además de esta evaluación de riesgos, hay dos pasos finales:

5) Aplicación de **medidas de mitigación** = *seleccionar y aplicar controles de seguridad para cada riesgo;*
6) Supervisión y reevaluación = *supervisar las amenazas y los riesgos a lo largo de cada etapa del ciclo de vida de los PDE y mantener actualizada la evaluación de riesgos.*

Para **los pasos uno a tres**, puede desarrollar una **matriz** que le permita clasificar cada amenaza, vulnerabilidad e impacto según el nivel de riesgo y la puntuación correspondientes. Para ello, primero debe definir qué significa cada nivel (y puntuación) para usted mediante tablas descriptivas[7]
.

- Bajo
- Bajo-medio
- Medio
- Medio-alto
- Alto

Tabla1 :
Matriz de ejemplo

Riesgo/Amenaza	Amenaza 1	Amenaza 2	Puntuación
Alto			10
Media-alta			
Media			
Bajo Medio			
Bajo			0

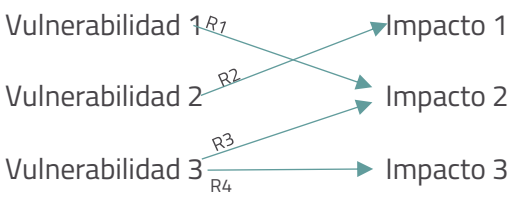
los principales pasos de cualquier enfoque de evaluación de riesgos. Se puede utilizar cualquier otro enfoque, norma o metodología, siempre que sea coherente con el enfoque descrito.

[7] Por ejemplo, en lo que respecta a la ocurrencia de amenazas, un nivel «bajo» podría significar una amenaza que puede producirse una vez cada diez años, mientras que un nivel «alto» podría significar una amenaza que puede producirse una vez a la semana. Se necesitan tablas descriptivas separadas para las amenazas, las vulnerabilidades y los impactos, y los riesgos; estos últimos sirven de apoyo a la definición de su nivel de aceptación.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

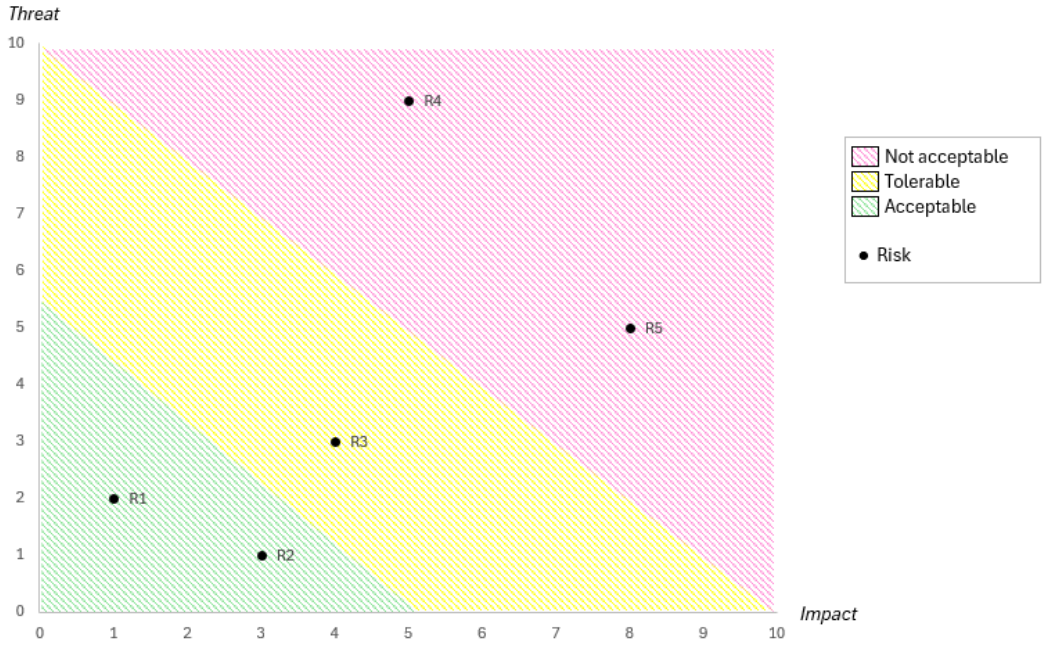
La vinculación de las vulnerabilidades con los impactos permite visualizar los diferentes riesgos (R):

Figura1 :
Visualización de riesgos



En **el cuarto paso**, es importante trazar los riesgos encontrados y definir su nivel de aceptación de dichos riesgos, lo que a menudo se hace mediante un código de colores, por ejemplo:

Figura2 :
Gráfico de aceptación de riesgos



Esto le permite priorizar dónde actuar y desarrollar medidas de mitigación y controles de seguridad para cada riesgo, con el fin de reducir los riesgos residuales a un nivel aceptable.

Como se ha indicado anteriormente, estos elementos de la evaluación de riesgos se tratan con mayor detalle a continuación (capítulo 1 de esta guía), proporcionando ejemplos y herramientas y marcos recomendados para ayudarle.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

1.1. Evaluación de los riesgos de ciberseguridad durante el ciclo de vida

Dado que los riesgos de ciberseguridad asociados a su PDE deben evaluarse a lo largo del ciclo de vida del producto, la realización de una **evaluación de riesgos de ciberseguridad durante el ciclo de vida** implica **identificar, analizar y mitigar los riesgos de ciberseguridad** en cada etapa del ciclo de vida de un producto:

1. Diseño
2. Desarrollo
3. Producción
4. Implementación
5. Operación y mantenimiento
6. Fin de vida útil (EOL)

La evaluación de riesgos debe actualizarse continuamente durante todo el «período de soporte»[8] , un período de al menos cinco años (o, si la vida útil del producto es inferior a cinco años, al menos hasta el final de la vida útil del producto).

1.1.1. Pasos clave en la evaluación de riesgos del ciclo de vida

A la hora de realizar la evaluación de riesgos, se pueden tener en cuenta seis pasos, cada uno de los cuales se aclara en la tabla 2 que figura a continuación.

Tabla2 :
Pasos clave en la evaluación del riesgo del ciclo de vida

Paso clave	Aclaración y sugerencias
1. Identificar activos y amenazas	Distinguir entre: • Activos: ¿qué necesita protección? Por ejemplo, firmware, datos de usuario, canales de comunicación.

[8] Artículo 13, apartado 8, del Reglamento sobre los productos de consumo: Los fabricantes determinarán el período de soporte de manera que refleje el período de tiempo durante el cual se prevé que vaya a utilizarse el producto, teniendo en cuenta, en particular, las expectativas razonables de los usuarios, la naturaleza del producto —incluida su finalidad prevista— y el Derecho pertinente de la Unión que fija la vida útil del producto con elementos digitales.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

	• Amenazas: ¿qué podría salir mal? Por ejemplo, inyección de malware, acceso no autorizado.
2. Analizar vulnerabilidades	Utilizar herramientas como: • Análisis de código estático; • Análisis de composición de software (SCA); • Realización de pentests; • Modelado de amenazas[9] (por ejemplo, STRIDE, DREAD). Nota: CVSS y STRIDE se pueden utilizar conjuntamente en un proceso de modelización de amenazas. STRIDE puede ayudar a identificar amenazas potenciales y CVSS se puede utilizar para evaluar la gravedad de las vulnerabilidades relacionadas con esas amenazas, lo que permite priorizar mejor las medidas de mitigación[10] .
3. Evaluar el impacto y la probabilidad del riesgo	Utilice una matriz de riesgos para establecer prioridades en función de: • El impacto (por ejemplo, violación de la seguridad de los datos, fallo/caída del sistema); • Probabilidad (por ejemplo, vulnerabilidad conocida, superficie de ataque).
4. Analice los riesgos y su aceptabilidad	Defina su nivel de aceptación y trace sus riesgos según la amenaza y el impacto para clasificar y priorizar sus acciones.
5. Implemente medidas de mitigación	Aplique controles de seguridad: por ejemplo, cifrado, autenticación, arranque seguro.
6. Supervise y reevalúe	Supervise continuamente las nuevas amenazas y actualice las evaluaciones de riesgos en consecuencia.

[9] El modelado de amenazas se analiza con más detalle en el punto 1.3.1.

[10] El CVSS evalúa la gravedad de la vulnerabilidad, mientras que el riesgo también tiene en cuenta el impacto en el negocio y la probabilidad.

1.1.2. Casos de uso por etapa del ciclo de vida

Para que la evaluación de riesgos del ciclo de vida sea más tangible, la tabla 3 que figura a continuación ofrece una visión general de los casos de uso, incluyendo un ejemplo de riesgo y una estrategia de mitigación, por etapa del ciclo de vida.

Tabla3 :
Casos de uso por etapa del ciclo de vida

Etapa del ciclo de vida	Caso de uso	Riesgo	Mitigación
Diseño	Cámara inteligente para el hogar	Acceso no autorizado a las transmisiones de vídeo	Implementar cifrado de extremo a extremo y configuración predeterminada segura
Desarrollo	Firmware del dispositivo	Vulnerabilidad de desbordamiento del búfer	Utilizar prácticas de codificación seguras y análisis automatizado de vulnerabilidades.
Producción	Pasarela IoT industrial	Compromiso durante la fabricación	Cadena de suministro segura y raíz de confianza de hardware, sellos de evidencia de manipulación y aprovisionamiento seguro
Implementación	Router de consumo	Las credenciales predeterminadas no se modifican	Forzar el cambio de contraseña obligatorio en el primer uso
Operación y mantenimiento	Vehículo conectado	Vulnerabilidades de software sin parchear	Actualizaciones OTA (Over-The-Air) con comprobaciones de integridad
Fin de vida útil	Termostato inteligente	Dispositivo abandonado con firmware explotable	Proporcionar instrucciones seguras para el desmantelamiento y el borrado de datos, política de actualización de seguridad al

			final de la vida útil y exportación de datos para los usuarios

1.1.3. Herramientas y marcos de trabajo para ayudarle

La siguiente lista destaca varias herramientas y marcos que pueden proporcionar apoyo, aunque todavía se está elaborando una lista más exhaustiva y normas armonizadas.

- ISO/IEC 27005: gestión de riesgos
- NIST SP 800-30: metodología de evaluación de riesgos
- ENISA Threat Landscape: información actualizada sobre amenazas
- OWASP ASVS: verificación de la seguridad de las aplicaciones
- Modelo STRIDE
- Modelo de evaluación de riesgos DREAD
- LINDDUN
- CVSS

1.2. Medidas de seguridad adaptadas

La segunda dimensión de un enfoque de ciberseguridad basado en el riesgo consiste en adaptar las medidas de seguridad al nivel de riesgo. La adaptación debe ser proporcional a los riesgos identificados en el anexo I, parte I(1). Analicemos lo que esto significa con seis pasos claros, principios y dos ejemplos de productos: un termostato inteligente (riesgo bajo a moderado) y un sistema de control industrial (ICS) (riesgo alto).

1.2.1. Realizar la clasificación de riesgos del producto

Al realizar una evaluación de riesgos específica del producto, es importante tener en cuenta las siguientes dimensiones.

- **Exposición a amenazas**: El producto...
  - ¿Está conectado a Internet?
  - ¿Está ampliamente implantado?

- ¿Está expuesto al público?
- ¿Uso previsto frente a uso indebido razonablemente previsible?

- **Impacto de la vulnerabilidad**: ¿Cuál sería el impacto en la seguridad, las pérdidas financieras, la privacidad y las infraestructuras críticas?
- **Atractivo para sufrir ataques:** ¿Sería un trampolín para movimientos laterales posteriores?
- **Perfil del usuario:** ¿consumidor, PYME, operador de infraestructura crítica?

En base a estas consideraciones, el producto puede clasificarse como de riesgo bajo (aceptable), riesgo moderado (tolerable) o riesgo alto (inaceptable)[11] .

1.2.2. Definir los objetivos de seguridad según el nivel de riesgo

La tabla 4 ilustra cómo se pueden adaptar los objetivos de seguridad al nivel de riesgo del producto establecido previamente.

Tabla4 :
Objetivos de seguridad por nivel de riesgo

Nivel de riesgo	Objetivos de seguridad
Bajo (por ejemplo, termostato inteligente)	• Evitar el uso indebido trivial. • Garantizar la privacidad. • Mantener la capacidad de actualización.
Moderado	• Detectar y mitigar vectores de ataque conocidos; • Reforzar la autenticación. • Garantizar la seguridad de las comunicaciones.
Alta (por ejemplo, ICS)	• Fortalecer la postura de seguridad. • Defensa en profundidad. • Confianza en la cadena de suministro; • Arranque seguro;

[11] Esto requiere que se defina de antemano cómo puntuar estos elementos utilizando una matriz y cómo las puntuaciones se corresponden con los niveles de riesgo. Para una clasificación más precisa, se pueden considerar cinco niveles de riesgo en lugar de tres: riesgo bajo, medio-bajo, medio, medio-alto y alto.

	• Supervisión de incidentes.

1.2.3. Asignación de los requisitos esenciales de la CRA al nivel de riesgo

Dependiendo del nivel de riesgo, los requisitos esenciales de la CRA pueden tener diferentes aplicaciones prácticas. La tabla 5 ilustra esto para los niveles de riesgo bajo y alto y los respectivos casos de productos de ejemplo, el termostato inteligente y el ICS.

Tabla5 :
Requisitos esenciales de la CRA por nivel de riesgo

Requisito CRA	Riesgo bajo	Riesgo alto
Seguridad por diseño y por defecto	Desactivar los puertos de depuración; valores sólidos predeterminados	Lista completa de materiales de software (SBOM[12]); arranque seguro; sistema operativo reforzado
Gestión de vulnerabilidades	Política pública de CVD; security.txt; supervisión de la bandeja de entrada; mecanismo de parches	Divulgación coordinada; PSIRT; respuesta rápida
Registro y supervisión	Registros de eventos locales	Registro remoto; integración SIEM
Control de acceso	Autenticación mediante PIN o aplicación	Acceso basado en roles; MFA; privilegios mínimos
Mecanismo de actualización	Actualizaciones OTA con el consentimiento del usuario	Actualizaciones firmadas; reversión a prueba de fallos
Protección contra el acceso no autorizado	Reglas básicas de firewall	Sistemas de detección de intrusiones en el host; comprobaciones de integridad del firmware

[12] La SBOM se aclara con más detalle en la sección 4.1.

1.2.4. Utilizar modelos de amenazas para perfeccionar las medidas

Para el modelado de amenazas, se pueden aplicar STRIDE, LINDDUN o árboles de ataque para validar la adecuación de los controles.

Para los casos de productos de ejemplo, esto significa:

- **Termostato inteligente**: centrarse en la suplantación de identidad, la manipulación y la denegación de servicio.
- **ICS**: cubrir todas las amenazas STRIDE y las amenazas persistentes avanzadas (APT).

1.2.5. Seleccionar controles por nivel de riesgo

La tabla 6 sugiere diferentes controles por dominio de seguridad para los casos prácticos de ejemplo, termostato inteligente (riesgo bajo) y ICS (riesgo alto).

Tabla6 :
Controles por nivel de riesgo

Ámbito de seguridad	Riesgo bajo	Riesgo alto
Autenticación	Autenticación basada en aplicaciones; cambio de contraseña predeterminada	MFA; control de acceso basado en certificados
Seguridad del firmware	Firmware firmado; actualizaciones OTA; reversión a prueba de fallos	Arranque seguro; integración TPM; garantía de la cadena de suministro
Comunicación	HTTPS/TLS	VPN; IPSec; segmentación de red; zero-trust
Supervisión	Rotación básica de registros	Registro en tiempo real; detección de anomalías; integración SOC; registros sincronizados en el tiempo
Interfaz de usuario	Panel de configuración sencillo	Consola de administración detallada; capacidades de seguimiento de auditoría

1.2.6. Pruebas de cumplimiento normativo

Como se ha indicado anteriormente, un elemento clave para el cumplimiento de la CRA es documentar, como mínimo, las siguientes pruebas:

- Justificación de la clasificación de riesgos.
- Decisiones de control vinculadas a los riesgos;
- Resultados de pruebas y validaciones;
- Políticas de actualización y gestión de vulnerabilidades;
- Alineación del ciclo de vida del desarrollo seguro (por ejemplo, ISO/IEC 27034, IEC 62443-4-1);
- Matriz de trazabilidad que relaciona riesgos → controles → pruebas de verificación → pruebas (que se conservarán en la documentación técnica)

1.2.7. Ejemplos

La tabla 7 ofrece ejemplos adicionales de medidas de implementación para los casos prácticos de riesgo bajo y alto.

Tabla7 :
Medidas de implementación por nivel de riesgo

Producto	Termostato inteligente	ICS
Consideraciones de riesgo	• Conectado a Internet, controla la calefacción en viviendas particulares. • Sensible a la privacidad, pero con bajo impacto en la seguridad o la economía.	• Se utiliza en infraestructuras críticas (por ejemplo, tratamiento de aguas). • Alto impacto en la seguridad y el funcionamiento.
Clasificación del riesgo	Riesgo bajo	Riesgo alto

Medidas de implementación	• Cambiar la contraseña predeterminada en el primer uso. • Comunicación HTTPS con el backend. • Actualizaciones de firmware firmadas; • Logs/Registros únicamente en local[13] ; • Formulario básico de contacto para vulnerabilidades.	• Hardware seguro por diseño con TPM; • Arranque seguro y actualizaciones firmadas con rollback; • Acceso basado en roles y MFA; • Segmentación de red y reglas de firewall; • Registro en SIEM central; • SBOM completo con cada actualización; • Proceso coordinado de divulgación de vulnerabilidades (CVD);

1.3. Consideración de modelos de amenazas, superficies de ataque y posible impacto en los usuarios y los sistemas.

La CRA hace hincapié en un enfoque de la ciberseguridad basado en el riesgo. Como se ha mostrado anteriormente, esto significa que los fabricantes deben adaptar sus medidas de seguridad a las amenazas reales, los puntos de exposición y las posibles consecuencias para los usuarios y los sistemas. No se trata de una directiva vacía, sino de un llamamiento a adoptar un enfoque fundamentado y consciente del contexto. Para aplicar eficazmente esta obligación, deben tenerse en cuenta conjuntamente tres conceptos clave: los modelos de amenaza, las superficies de ataque y el análisis de impacto, que conforman la tercera y última dimensión del enfoque de la ciberseguridad basado en el riesgo. A continuación, se examinan estos elementos uno por uno y para ver cómo encajan entre sí.

[13] Nota: La tenencia de logs únicamente en local reduce el valor forense, por lo que se recomienda la exportación opcional con el consentimiento del usuario.

1.3.1. Modelos de amenazas: ¿Quién ataca, por qué y cómo?

El modelado de amenazas es un proceso estructurado en el que se identifica quién podría atacar su producto, cómo lo haría y cuál sería su motivación. Piense en los "script kiddies" (personas que realizan ataques informáticos utilizando herramientas y scripts creados por otros), los ciberdelincuentes organizados o incluso los actores estatales. Sus motivos varían desde el lucro económico hasta el sabotaje o el espionaje, y sus habilidades van desde las más básicas hasta las más avanzadas.

Para estructurar esto, puede utilizar métodos como:

- STRIDE;
- MITRE ATT&CK para técnicas de ataque conocidas;
- LINDDUN para amenazas orientadas a la privacidad;
- "Attacks trees" o "Cyber Kill chains" para mapear las rutas de ataque.

Volviendo a los casos prácticos, esto significa:

- **Termostato inteligente**: las amenazas suelen limitarse a vecinos curiosos o ataques aleatorios, en los que alguien podría manipular los ajustes de temperatura o el consumo de energía;
- **ICS** (por ejemplo, en una planta de tratamiento de agua): las amenazas son fundamentalmente diferentes, por ejemplo, los grupos APT o las bandas de ransomware intentan sabotear los procesos físicos o cerrar un negocio.

El resultado del modelado de amenazas es una lista clara de objetivos de seguridad específicos para el producto y su entorno.

1.3.2 Superficies de ataque: ¿por dónde puede entrar un atacante?

Una superficie de ataque es la totalidad de todos los puntos en los que un atacante puede interactuar con el sistema o influir en él. Cuantas más interfaces y puntos de acceso, mayor es el riesgo.

Las superficies de ataque típicas son:

- Interfaces de red como Wi-Fi, Bluetooth, MQTT o HTTP;
- Interfaces locales como USB, UART, JTAG (para depuración);
- Mecanismos de actualización como OTA o actualizaciones USB;
- API, aplicaciones móviles, paneles de control en la nube:

- Componentes externos de la cadena de suministro.

El análisis de estas superficies implica comprobar qué componentes están expuestos innecesariamente, qué servicios están habilitados pero no son necesarios y si el acceso está protegido adecuadamente. Lo ideal es limitar la superficie de ataque mediante:

- Principios de seguridad como la exposición mínima, los valores predeterminados seguros y el bastionado/hardnening;
- Desactivar los puertos o servicios que no se utilizan;
- Autenticación y cifrado en todas las interfaces.

Aplicado a los ejemplos, esto significa:

- **Termostato inteligente**: normalmente utilizará Wi-Fi y posiblemente Bluetooth, con una simple conexión a la nube. Las interfaces de depuración pueden estar abiertas durante las pruebas y deben desactivarse en producción.
- **Pasarela ICS**: estará protegida físicamente, con actualizaciones USB blindadas, redes segmentadas y sin interfaces externas.

Por lo tanto, es esencial realizar un mapeo cuidadoso de la superficie de ataque para saber dónde se necesita realmente la seguridad.

1.3.3 Análisis de impacto: ¿qué ocurre si las cosas salen mal?

El último paso es determinar el impacto potencial de un ataque exitoso. La CRA exige que las medidas de seguridad sean proporcionales a este impacto. Esto incluye no solo los daños técnicos, sino también:

- Peligros para el usuario (por ejemplo, lesiones debidas al control de la temperatura);
- Violación de la privacidad (por ejemplo, deducir patrones de vida a partir de los datos del termostato);
- Pérdida de disponibilidad o continuidad del negocio (por ejemplo, cierre de la fábrica);
- Responsabilidad legal (por ejemplo, violación de la CRA o el RGPD);
- Daño a la reputación y riesgo de mercado.

El impacto debe considerarse en múltiples dimensiones:

- Usuario: desde inconvenientes menores hasta situaciones que ponen en peligro la vida;
- Organización: desde un aumento de la carga de trabajo del servicio de asistencia técnica hasta la interrupción de la actividad empresarial;
- Sociedad: desde errores inocentes hasta amenazas a infraestructuras críticas.

También en este caso, la proporcionalidad es clave: un robot de juguete no requiere el mismo nivel de seguridad que una bomba médica de infusión.

1.3.4 Integración: del análisis a las medidas

Cuando estos tres pilares se unen (modelo de amenazas, superficie de ataque e impacto), se crea una base sólida para adaptar las medidas de seguridad.

Un enfoque típico es el siguiente:

1. Definir el uso y el contexto del producto.
2. Realizar un modelo de amenazas para comprender a los actores, los motivos y las vías de ataque.
3. Mapear la superficie de ataque e identificar las vulnerabilidades.
4. Analizar el impacto en los usuarios, las organizaciones y la sociedad.
5. Seleccionar medidas basadas en el riesgo (riesgo = probabilidad × impacto).
6. Documentar todo para cumplir con los requisitos de la CRA y las auditorías.

En los casos prácticos, esto significa:

- **Termostato inteligente**: cuenta con cifrado, una política de contraseñas seguras, actualizaciones OTA firmadas y una declaración de privacidad sencilla.
- **Puerta de enlace ICS**: obtiene arranque seguro, raíz de confianza de hardware, redes segmentadas, registro SIEM, gestión de roles y un SBOM completo con supervisión de vulnerabilidades.

2. Diseño y desarrollo seguros

Volviendo al punto 1 del anexo I, parte I, de la CRA, el enfoque de ciberseguridad basado en el riesgo y la adaptación se basa en el principio de «seguridad por diseño y por defecto», es decir, los PDE deben diseñarse y desarrollarse para que sean seguros desde el principio. Ya no basta con añadir la seguridad como una capa opcional a posteriori, sino que debe ser una parte esencial de todo el proceso de desarrollo del producto.

La «seguridad desde el diseño», la «seguridad por defecto» y el uso de prácticas de desarrollo seguras constituyen el núcleo de una estrategia de productos digitales resilientes. Garantizan que la seguridad no sea una idea de último recurso, sino una parte estructural y demostrablemente integrada en el producto, tal y como exige la CRA.

Mediante el uso de normas internacionales como IEC 62443, ISO 27034, OWASP y las directrices de ENISA, los fabricantes pueden aplicar estos principios de manera eficiente y cumplir al mismo tiempo con sus obligaciones de conformidad.

Los productos deben ser:

1. **"Secure by design"**: la seguridad se integra desde las primeras etapas del desarrollo.
2. **"Secure by default"**: la configuración predeterminada debe dar prioridad a la seguridad (por ejemplo, contraseñas seguras, mínimo número de puertos abiertos, etc.).
3. **Desarrollados de forma segura**: utilizando prácticas de codificación seguras y modelos de amenazas.

2.1. "Secure by design": seguros desde el diseño inicial

«Seguridad desde el diseño» significa que la ciberseguridad se tiene en cuenta desde la fase conceptual en las decisiones sobre la arquitectura, la selección de componentes y la interacción entre subsistemas. La seguridad debe ser tan fundamental como la funcionalidad o la facilidad de uso.

Ejemplo práctico:

Al diseñar un módulo de cerradura inteligente, se toman inmediatamente las siguientes decisiones:

- Aplicar el cifrado de extremo a extremo entre la aplicación y la cerradura.
- Almacenar las claves de forma segura en un TPM o elemento seguro.
- Desactivar físicamente los puertos de depuración después de la producción.

Las normas y directrices pertinentes a este respecto incluyen:

- IEC 62443-4-1: Requiere la integración de la seguridad en el ciclo de vida del software.
- ISO/IEC 27034: Seguridad de las aplicaciones en el ciclo de vida del desarrollo de software.
- NIST SP 800-218 SSDF.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- Buenas prácticas de desarrollo de software seguro de la ENISA.

2.2. "Secure by default": seguridad sin configuración por parte del usuario

«Seguridad por defecto» significa que los productos se entregan con la configuración más segura como estándar. El usuario no debería tener que adivinar si la seguridad está habilitada. La seguridad es la base, no una «configuración avanzada» opcional.

Ejemplos de configuraciones seguras por defecto:

- Sin valores predeterminados compartidos, forzar al hacer login por primera vez a una configuración de credenciales o vinculación/emparejamiento sin contraseña mediante métodos seguros (biometría, tokens, etc...).
- Solo se abren los puertos de red necesarios (principio de exposición mínima).
- Actualizaciones de firmware firmadas y verificadas de forma predeterminada.
- Registro y pista de auditoría habilitados de forma predeterminada para funciones críticas.

Las directrices pertinentes a este respecto incluyen:

- Configuración segura de OWASP: mejores prácticas para una configuración predeterminada segura.
- NIST SP 800-128: Guía para la gestión de la configuración centrada en la seguridad.

2.3. Prácticas de codificación segura

La CRA exige que el desarrollo de software se lleve a cabo de acuerdo con prácticas de desarrollo seguras y probadas, prestando atención continua a las amenazas. Esto significa, entre otras cosas:

Codificación segura:

- Validación de entradas (contra inyecciones SQL, desbordamientos de búfer, etc.).
- Uso de bibliotecas seguras y cifrado.
- Análisis de código estático y fuzz testing (también llamado fuzzing, pruebas que consisten en introducir datos aleatorios e inválidos en un programa para intentar que falle).

Modelado de amenazas:

Para cada componente del software, se debe evaluar lo siguiente:

- ¿Quién podría atacarlo?
- ¿Cómo podrían hacerlo?
- ¿Cuál sería el impacto?

Marcos como STRIDE (Microsoft), OWASP Threat Dragon y MITRE ATT&CK pueden ayudar a identificar sistemáticamente las vulnerabilidades y las vías de ataque.

Las normas y directrices pertinentes a este respecto incluyen:

- Lista de verificación de prácticas de codificación segura de OWASP;
- ISO/IEC 27001 Anexo A.14: Requisitos de seguridad en el desarrollo;
- Directrices de modelización de amenazas de la ENISA (2022);
- BSI TR-03161 (Alemania): Desarrollo de software seguro.

2.4. En términos concretos para los fabricantes

En resumen, una organización que desee desarrollar PDE que cumplan con la norma CRA debe:

- Adoptar un ciclo de vida de desarrollo de software seguro (SSDLC), tal y como se describe en la norma IEC 62443-4-1 o en la norma NIST SP 800-218 SSDF.
- Contar con una política de revisión y prueba de código que se centre en las vulnerabilidades (SAST, DAST, fuzzing);
- Aplicar sistemáticamente modelos de amenazas a todos los componentes importantes.
- Entregar productos con puertos cerrados estándar, registro habilitado y puertos de acceso seguros.
- Adoptar una función PSIRT con roles claros y procesos de guardia.
- Definir puertas de calidad de seguridad en CI/CD (SAST, DAST, SCA, secret scans) con políticas fail-the-build.

3. Gestión de la seguridad del ciclo de vida

Más allá del diseño, el desarrollo y la producción seguros de los PDE, su producto también debe permanecer seguro durante todo su ciclo de vida. Los productos digitales evolucionan, y su

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

seguridad también debe hacerlo. Esto significa que la seguridad debe gestionarse y tenerse en cuenta de forma continua, incluso después de que el PDE haya salido al mercado.

En concreto, los fabricantes deben gestionar[14]:

1. Supervisar continuamente las vulnerabilidades.
2. Proporcionar actualizaciones y parches de seguridad oportunos.
3. Mantener una política de divulgación de vulnerabilidades y comunicar los riesgos de forma transparente a los usuarios y a los reguladores.

3.1. Supervisión continua de vulnerabilidades

Una vez que un producto se comercializa, los fabricantes deben seguir detectando vulnerabilidades de forma activa y sistemática. Esto incluye:

- Supervisar bases de datos de vulnerabilidades, como la base de datos europea de vulnerabilidades[15] ;
- Supervisar los avisos de los proveedores.
- El seguimiento de las vulnerabilidades y exposiciones comunes (CVE) relacionadas con los componentes o bibliotecas utilizados;
- El uso de SBOM para identificar y rastrear dependencias;
- Supervisar internamente las nuevas vulnerabilidades mediante programas "bug bounty", pentests o auditorías de seguridad.

Ejemplo:

Un fabricante de cámaras en red utiliza módulos de firmware de código abierto. La base de datos CVE revela que uno de estos módulos contiene una vulnerabilidad crítica (por ejemplo, CVE-2023-XXXXX). El fabricante está obligado a supervisar y evaluar esta información y, si procede, tomar las medidas adecuadas.

[14] Aunque los requisitos para el tratamiento de las vulnerabilidades se tratan en profundidad en el anexo I, parte II, se derivan de los puntos 1 y 2 del anexo I, parte I, y, por lo tanto, ya se han abordado en la presente guía.

[15] Art. 17(5), CRA.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Las fuentes relevantes a este respecto incluyen:

- CVE.
- EPSS (Sistema de puntuación de predicción de exploits).
- Directrices de gestión de vulnerabilidades de la ENISA.
- ISO/IEC 30111: Procesos de gestión de vulnerabilidades.

3.2. Actualizaciones y parches de seguridad oportunos

La CRA exige a los fabricantes que respondan rápidamente a las vulnerabilidades conocidas y que distribuyan actualizaciones de seguridad de forma gratuita y eficaz durante todo el periodo de asistencia técnica.

Estas actualizaciones deben:

- Estar firmadas y validadas digitalmente.
- Contar con un mecanismo de rollback.
- Ser instalables automáticamente con opciones de exclusión voluntaria (opt-out options) y/o con una interacción mínima por parte del usuario.
- Permanecer disponibles durante al menos 10 años después de su lanzamiento, o durante el resto del período de soporte (la opción que dure más).

Ejemplo:

Un fabricante de termostatos inteligentes descubre una vulnerabilidad en la pila Wi-Fi. En dos semanas, se desarrolla, prueba y distribuye un parche de seguridad a través de una actualización OTA firmada. Los usuarios reciben una notificación clara y la actualización se instala automáticamente cuando se reinicia el dispositivo.

Las fuentes relevantes a este respecto incluyen:

- ISO/IEC 29147: Divulgación coordinada de vulnerabilidades;
- NIST SP 800-40: Guía para la gestión de parches en la empresa;
- ETSI EN 303 645: Base de referencia de seguridad para el IoT de consumo (incluidos los mecanismos de actualización de software).

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

3.3. Política de notificación de vulnerabilidades y comunicación transparente

La transparencia es esencial. La CRA exige a los fabricantes que:

- Publicación de una política de divulgación coordinada de vulnerabilidades (CVD);
- Proporcionen un punto de contacto (por ejemplo, security@company.eu) para la notificación de informes;
- Informar rápidamente a los usuarios y a las autoridades, como la ENISA o la autoridad nacional de supervisión, en caso de riesgos graves;
- Comunicar de forma transparente los parches disponibles, las medidas de mitigación y los riesgos restantes.

Ejemplo:

Un hacker ético informa de una vulnerabilidad crítica en un sistema de alarma conectado a través de la plataforma pública CVD del fabricante. En un plazo de 72 horas, se confirma la recepción y, tras un análisis interno, se informa a la ENISA a través de la plataforma única de notificación de la ENISA (endpoints nacionales). En un plazo de tres semanas se lanza un parche y se notifica a todos los usuarios el riesgo y la solución por correo electrónico y mediante notificaciones de la aplicación.

Las fuentes relevantes a este respecto incluyen:

- FIRST Vulnerability Coordination Maturity Model (VCMM);
- ISO/IEC 29147: Directrices para la divulgación de vulnerabilidades;
- Directrices de la ENISA para la divulgación coordinada de vulnerabilidades (2022);
- OpenSSF VEX (Intercambio de vulnerabilidades explotables).

4. Seguridad de la cadena de suministro

La CRA reconoce que un producto nunca es completamente «independiente»: está compuesto por docenas, a veces cientos, de componentes procedentes de proveedores externos, proyectos de código abierto y socios de hardware. Por eso, la CRA establece requisitos explícitos para gestionar los riesgos de ciberseguridad dentro de la cadena de suministro.

En la práctica, los fabricantes deben:

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

1. Mantener una visión general actualizada y transparente de los componentes de software utilizados a través de un SBOM;
2. Exigir a los proveedores que cumplan con la seguridad conforme a la CRA;
3. Supervisar y gestionar activamente los riesgos asociados al código abierto y a las dependencias externas.

4.1. Lista de materiales de software (SBOM)

Una SBOM es similar a una lista de ingredientes para software: contiene una descripción general de todos los componentes, versiones y orígenes de los elementos de software utilizados, incluidas las bibliotecas de código abierto.

La CRA exige a los fabricantes que mantengan una SBOM y que puedan presentarla a los reguladores y autoridades cuando lo soliciten. La publicación de la SBOM para los usuarios es opcional[16] . Esta SBOM constituye la base para:

- Análisis de vulnerabilidades (por ejemplo, mediante el seguimiento de CVE);
- La evaluación del impacto en caso de vulnerabilidades de día cero;
- Auditorías de la cadena de suministro.

Ejemplo:

Un fabricante de routers inteligentes elabora una SBOM en la que se indica claramente que el producto utiliza:

- OpenSSL 1.1.1n;
- BusyBox 1.35.0;
- Una versión modificada de un módulo de firewall de código abierto.

Cuando se divulga una vulnerabilidad en OpenSSL (CVE-2022-XXXX), el fabricante puede comprobar inmediatamente si el producto se ve afectado y responder de forma adecuada.

Las fuentes relevantes a este respecto incluyen:

- CycloneDX, SPDX: formatos SBOM (también recomendados por ENISA y NTIA);
- ISO/IEC 5230 (OpenChain): Cumplimiento del software de la cadena de suministro;

[16] Si se pone a disposición de los usuarios, aclare dónde y cómo pueden acceder a ella.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- Herramientas OpenSSF para la generación de SBOM y la detección de vulnerabilidades.

4.2. Requisitos de seguridad para los proveedores

La CRA también exige a los fabricantes que se aseguren de que sus proveedores y desarrolladores externos cumplan requisitos de seguridad comparables a los de su propio equipo. La responsabilidad no se puede delegar; las vulnerabilidades en componentes de terceros también pueden dar lugar a obligaciones de cumplimiento de la CRA.

En términos concretos, esto significa:

- Inclusión de cláusulas de ciberseguridad en los contratos con los proveedores.
- Realizar la debida diligencia en materia de seguridad al seleccionar proveedores de software.
- Verificar periódicamente que los socios cumplen, por ejemplo:
    - ISO/IEC 27001 (seguridad de la información);
    - IEC 62443-4-1 (desarrollo seguro de productos);
    - Modelos de madurez OWASP SAMM o BSIMM.
- Derechos de auditoría contractual y niveles mínimos de garantía (por ejemplo, certificación de declaraciones de conformidad) para componentes críticos.
- Notificación en un plazo de 24 horas de las vulnerabilidades críticas detectadas por los proveedores que afecten a sus PDE.

Ejemplo:

Un fabricante de dispositivos médicos IoT trabaja con un proveedor de software en Asia. El contrato estipula que este proveedor:

- Desarrolle de forma segura de acuerdo con la norma IEC 62443-4-1;
- Documente todos los componentes de código abierto utilizados;
- Mantenga una política de vulnerabilidad con notificación obligatoria en un plazo de 24 horas.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

4.3. Gestión de riesgos de bibliotecas de código abierto y externas

El software de código abierto ofrece muchas ventajas, pero también conlleva riesgos: vulnerabilidades, actualizaciones pendientes, licencias poco claras o mantenedores poco fiables. La CRA exige a los fabricantes que gestionen y supervisen activamente estos riesgos.

Las mejores prácticas incluyen:

- Utilizar escáneres de dependencias (por ejemplo, OWASP Dependency-Check, Snyk, Trivy);
- Alertas automáticas de vulnerabilidades (por ejemplo, a través de GitHub Advisories);
- Utilice únicamente proyectos de código abierto mantenidos y maduros.
- Aplique controles de seguridad en los procesos de CI/CD (bloqueando las compilaciones con CVE conocidos);
- Utilice VEX para reducir el ruido de las CVE no explotables.
- Exigir una capacidad de respuesta mínima por parte de los mantenedores al seleccionar OSS.

Ejemplo:

Un fabricante utiliza una biblioteca JavaScript popular (por ejemplo, Log4j) en una interfaz web. Al descubrir Log4Shell (CVE-2021-44228), el fabricante sabe exactamente qué versiones se ven afectadas mediante el análisis SBOM y puede segmentar y parchear los productos afectados.

Las fuentes relevantes a este respecto incluyen:

- NIST SSDF (Marco de desarrollo de software seguro);
- Directrices de seguridad de OSS de ENISA;
- OpenSSF Scorecard: evaluación objetiva de la calidad de los proyectos de código abierto.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Conclusión

Esta guía presenta una primera **traducción técnica de los requisitos del anexo I, parte I**, **de la CRA en sugerencias y recomendaciones prácticas**. Destaca **cuatro componentes** que son fundamentales para el cumplimiento de la CRA: (1) un enfoque de ciberseguridad basado en el riesgo, que implica una evaluación de riesgos, medidas de seguridad adaptadas y una consideración de los modelos de amenazas, las superficies de ataque y los impactos; (2) el principio de seguridad desde el diseño/por defecto; (3) las obligaciones de gestión de la seguridad a lo largo del ciclo de vida de su PDE; (4) consideraciones y controles de la cadena de suministro. Para cada componente, se ofrecen **sugerencias prácticas** sobre cómo implementar y cumplir con estas obligaciones basadas en las mejores prácticas y normas reconocidas. Sin embargo, estas están sujetas a cambios en función de los debates sobre las normas actuales y la evolución de la normativa. Como próximos pasos para las pymes, se recomienda consultar las directrices adicionales del **repositorio SECURE**, como el **Marco metodológico de evaluación del cumplimiento de la CRA**, que ofrece un conjunto de herramientas paso a paso y una lista de verificación sobre el cumplimiento de la CRA más allá del anexo I, así como **CRA 101: Comprender las obligaciones de la CRA**, que ofrece una visión general condensada y fácil de entender para principiantes sobre sus obligaciones legales en virtud de la CRA.