



Seguridad de la Cadena de Suministro de Software y Nueva Regulación

AMENAZAS, CONTROLES TÉCNICOS Y EL MARCO
NORMATIVO INTERNACIONAL

E-boletín Informativo CSIRT Académico
UNAD

Medio de divulgación: Correo Electrónico,
Sitio Web

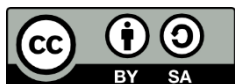
Incluye: Noticias, alertas o informes
relacionados con la disciplina de la
ciberseguridad

Número Cuarenta y tres [43]
Septiembre de 2026

Universidad Nacional Abierta y a Distancia
(UNAD)

Universidad Nacional Abierta y a Distancia
Calle 14 sur No. 14-23 | Bogotá D.C
Correo electrónico:
csirt@unad.edu.co
Página web: <https://csirt.unad.edu.co>

Licencia Atribución – Compartir igual



Estado legal:
Periodicidad: Mensual
ISSN: 2806-0164

Edición electrónica, financiada por la
Universidad Nacional Abierta y a
Distancia (UNAD)

Vicerrectoría de Innovación y
Emprendimiento (VIEM)
Ing. Andrés Ernesto Salinas
Vicerrector

Escuela de Ciencias Básicas Tecnología e
Ingeniería (ECBTI)
Ing. Claudio Camilo González Clavijo
Decano

Maestría en Ciberseguridad (ECBTI)
Ing. Sonia Ximena Moreno Molano
Líder de Programa

Especialización en Seguridad Informática
Ing. Cesar Antonio Villamizar
Líder de Programa

Semillero de Investigación Ceros y Unos,
adscrito al Grupo de Byte InDesign

Centro de Desarrollo Tecnológico CSIRT Académico UNAD

Ing. Luis Fernando Zambrano Hernández
Líder CSIRT Académico UNAD

Responsable de la Edición
Ing. Luis Fernando Zambrano Hernandez

Revisó
Adm. Libardo Cárdenas Corral
Analista CSIRT Académico UNAD

El software moderno ya no se escribe: se ensambla. Una aplicación típica integra cientos de bibliotecas de código abierto, servicios de terceros y herramientas de compilación automatizadas, de modo que su seguridad depende de una larga cadena de actores sobre los que la organización tiene poco control. Ataques como SolarWinds, la puerta trasera de XZ Utils o el gusano Shai-Hulud en npm demostraron que comprometer un solo eslabón permite alcanzar a miles de víctimas a la vez.

Este boletín académico presenta una revisión de la literatura científica y del marco normativo sobre la seguridad de la cadena de suministro de software, organizada en tres ejes temáticos: las amenazas y ataques representativos, los controles técnicos que permiten mitigarlos y la nueva regulación internacional, con especial atención al Cyber Resilience Act europeo, cuyas obligaciones de reporte entraron en vigor en septiembre de 2026.

Tabla de contenido

1. Introducción.....	4
2. Seguridad de la Cadena de Suministro de Software.....	6
2.1. Amenazas y ataques a la cadena de suministro de software.....	6
2.2. Controles técnicos: SBOM, firma y procedencia del software.....	8
2.3. Nueva regulación: Cyber Resilience Act, NIS2 y el enfoque de Estados Unidos	10
3. Conclusiones.....	14
4. Recomendaciones.....	15
5. Referentes Bibliográficos	16

1. Introducción

La cadena de suministro de software¹ se ha convertido en uno de los blancos preferidos de los atacantes porque ofrece un efecto multiplicador: en lugar de vulnerar a cada víctima por separado, basta con comprometer un componente, una cuenta de publicación o un sistema de compilación del que muchas organizaciones dependen. La literatura reciente documenta una amplia variedad de vectores de ataque que explotan precisamente las relaciones de confianza entre desarrolladores, repositorios, herramientas y consumidores de software (Ladisa et al., 2023; Williams et al., 2025).

La respuesta a este problema se ha dado en dos frentes. En el técnico, la comunidad ha desarrollado prácticas y herramientas como el inventario de componentes de software (SBOM)², la firma de artefactos y la verificación de su procedencia, cuya adopción, sin embargo, avanza con dificultades (Stalnaker et al., 2024; Zahan et al., 2023). En el normativo, los gobiernos han pasado de las recomendaciones voluntarias a las obligaciones legales: la Unión Europea aprobó el Cyber Resilience Act (CRA) y la Directiva NIS2, mientras que Estados Unidos ha ajustado varias veces su política de compras públicas de software seguro.

El propósito de este boletín es sintetizar el estado del conocimiento sobre la seguridad de la cadena de suministro de software y el nuevo marco regulatorio que la acompaña. El documento se estructura en tres ejes temáticos que van de la amenaza a la respuesta: primero, las etapas de la cadena y los ataques que las han afectado; segundo, los controles técnicos de transparencia, integridad y procedencia; y tercero, la regulación emergente en la Unión Europea y Estados Unidos, junto con sus implicaciones para las organizaciones latinoamericanas.

¹ Conjunto de personas, procesos, componentes, herramientas e infraestructura que intervienen desde la escritura del código hasta la entrega y actualización del software en manos del usuario.

² Software Bill of Materials: inventario formal y legible por máquina de los componentes, bibliotecas y dependencias que integran un producto de software, con sus versiones y relaciones.

Seguridad de la Cadena de Suministro de Software y Nueva Regulación

Amenazas, controles técnicos y el nuevo marco normativo internacional

Autores

Luis Fernando Zambrano Hernandez

Docente Investigador
Líder CSIRT Académico UNAD
Universidad Nacional Abierta y a Distancia
ORCID: 0000-0002-4690-3526

Hernando José Peña Hidalgo

Docente Investigador
CSIRT Académico UNAD
Universidad Nacional Abierta y a Distancia
ORCID: 0000-0002-3477-2645

Rosa María Zambrano Burbano

Analista CSIRT Académico UNAD
Universidad Nacional Abierta y a Distancia
ORCID: 0009-0005-3604-4288

Néstor Raúl Cárdenas Corral

Analista CSIRT Académico UNAD
Universidad Nacional Abierta y a Distancia
ORCID: orcid.org/0000-0003-3691-0148

2. Seguridad de la Cadena de Suministro de Software

2.1. Amenazas y ataques a la cadena de suministro de software

Un ataque a la cadena de suministro de software consiste en comprometer un eslabón intermedio, como el código fuente, una dependencia, el sistema de compilación o el canal de distribución, para que el código malicioso llegue a los usuarios finales a través de un canal en el que estos ya confían. Ladisa et al. (2023) sistematizaron este fenómeno en una taxonomía de 107 vectores de ataque y 33 salvaguardas, validada con 17 expertos y 134 desarrolladores, que evidencia que cada etapa de la cadena constituye una superficie de ataque con características propias.

El caso más estudiado es el de SolarWinds (2020), en el que los atacantes insertaron el código malicioso SUNBURST en el proceso de compilación de la plataforma Orion, de modo que fue distribuido como una actualización legítima y firmada a miles de clientes, entre ellos agencias gubernamentales. Martínez y Durán (2021) lo

describen como una amenaza a la ciberseguridad global y recomiendan, entre otras medidas, el uso de SBOM, la arquitectura de confianza cero, los lineamientos de NIST SP 800-161 y la autenticación multifactor.

Los repositorios de paquetes de código abierto son otro frente crítico. Ohm et al. (2020) analizaron

174 paquetes maliciosos publicados entre 2015 y 2019 en npm, PyPI y RubyGems, y modelaron en árboles de ataque las técnicas empleadas, como la suplantación de nombres de paquetes (*typosquatting*) y la toma de control de cuentas de mantenedores. Estas técnicas siguen vigentes: en septiembre de 2025, el gusano autopropagable Shai-Hulud comprometió más de 500 paquetes de npm y robó tokens de GitHub y credenciales de servicios en la nube³.

Los incidentes recientes muestran además una creciente sofisticación. En la biblioteca XZ Utils (CVE-2024-3094), un colaborador ganó durante años la confianza del proyecto antes de insertar una puerta trasera, y en el caso de 3CX (2023) la aplicación de escritorio fue troyanizada como consecuencia de un compromiso previo en otro proveedor,

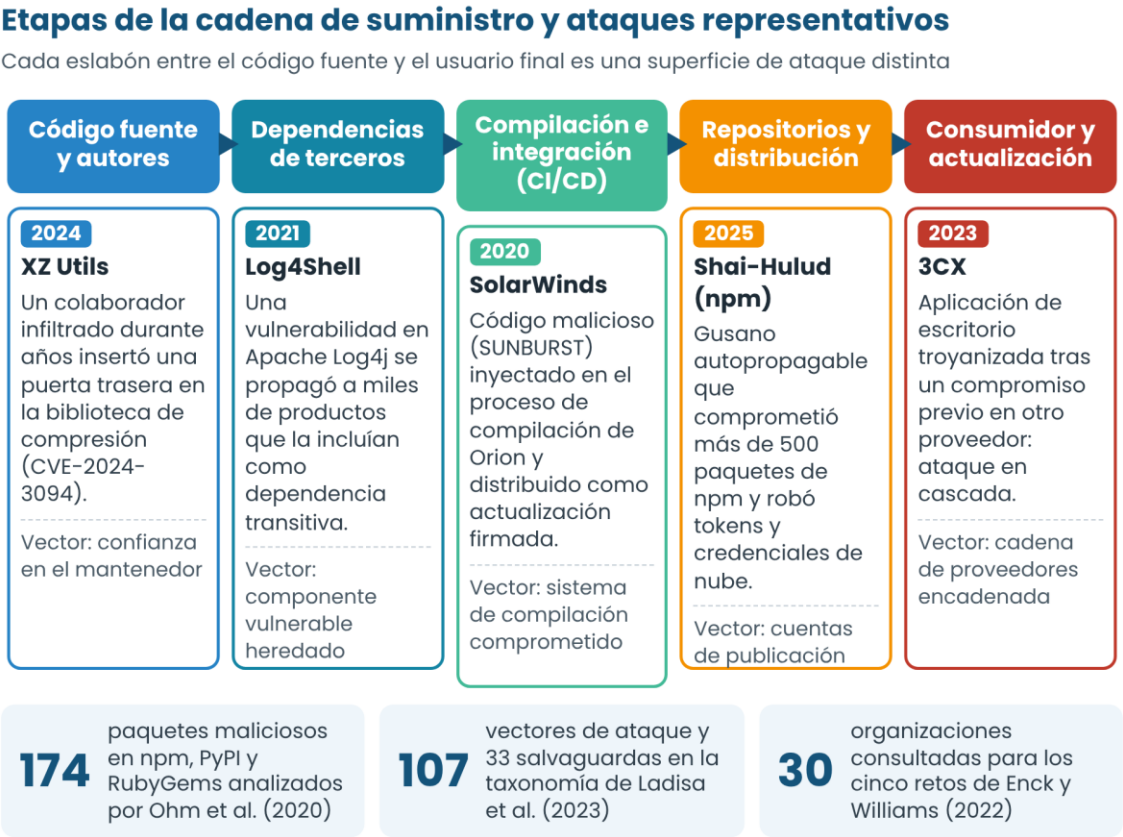
configurando un ataque en cascada. Vulnerabilidades no intencionales como Log4Shell (2021) ilustran, por su parte, cómo una sola dependencia transitiva puede exponer a miles de productos a la vez.

Desde la perspectiva de las organizaciones, Enck y Williams (2022) reunieron a 30 entidades de la industria y el gobierno e identificaron cinco retos prioritarios: actualizar las dependencias vulnerables, aprovechar el SBOM para la seguridad, elegir dependencias confiables, proteger el proceso de compilación y lograr la participación de toda la industria. Williams et al. (2025) amplían esta agenda y concluyen que la seguridad de la cadena exige soluciones que abarquen a todos sus actores y no solo al producto final.

³ Cybersecurity and Infrastructure Security Agency (CISA). Widespread Supply Chain Compromise Impacting npm Ecosystem (septiembre de 2025).

<https://www.cisa.gov/news-events/alerts/2025/09/23/widespread-supply-chain-compromise-impacting-npm-ecosystem>

Ilustración 1.
Etapas de la cadena de suministro de software y ataques representativos



Elaboración propia con base en Ladisa et al. (2023), Ohm et al. (2020), Enck y Williams (2022), Martínez y Durán (2021) y CISA³.

2.2. Controles técnicos: SBOM, firma y procedencia del software

Las respuestas técnicas convergen en tres propiedades de diseño seguro propuestas por Okafor et al. (2022): la transparencia, que permite conocer qué componentes, pasos y actores intervienen en la cadena; la validez, que asegura la integridad verificable de cada artefacto; y la separación, que aísla las etapas y limita los privilegios. Sobre esta base se articulan prácticas de proceso, como el marco de desarrollo seguro SSDF de NIST⁴, y controles sobre los artefactos, como el SBOM, la firma digital y la procedencia de la compilación.

⁴ National Institute of Standards and Technology (NIST). Secure Software Development Framework (SSDF), SP 800-218. <https://csrc.nist.gov/pubs/sp/800/218/final>

El SBOM es el control de transparencia más difundido, aunque su adopción dista de ser madura. Zahan et al. (2023) analizaron doscientos artículos y recursos en línea e identificaron los principales beneficios y desafíos de su uso, mientras que Xia et al. (2023) encontraron una brecha significativa entre la disponibilidad de herramientas de generación y su integración efectiva en la gestión de riesgos. Stalnaker et al. (2024), a partir de una encuesta a 138 profesionales, identificaron 12 retos principales en la creación y el uso de SBOM, y propusieron cuatro soluciones accionables.

La calidad del SBOM es otro problema recurrente. Balliu et al. (2023) documentaron, en el ecosistema Java, la resolución incompleta de dependencias transitivas y la falta de metadatos confiables. Una revisión sistemática de 40 estudios identificó 11 barreras de adopción y mostró que las herramientas de análisis pueden discrepar de forma notable: sobre el mismo conjunto de 1 151 SBOM, una herramienta reportó 309 022 vulnerabilidades y otra 43 553 (O'Donoghue et al.,

2025). Para reducir el ruido, el formato VEX⁵ permite al fabricante declarar si una vulnerabilidad de un componente es realmente explotable en su producto.

Los controles de validez se centran en la integridad y la procedencia de los artefactos. Sigstore propone la firma basada en identidad, en la que los desarrolladores firman con certificados de corta duración vinculados a su cuenta y cada firma queda registrada en un log público de transparencia, lo que elimina la gestión de llaves de larga duración (Newman et al., 2022). De forma complementaria, el marco SLSA⁶ define niveles de garantía para el proceso de compilación, y las atestaciones in-toto permiten verificar que cada paso de la cadena fue ejecutado por quien debía y en el orden previsto.

Ninguno de estos controles es suficiente por sí solo. Abu Ishgair et al. (2024) modelaron la cadena de suministro como un grafo con 21 objetivos de seguridad, evaluaron 27 enfoques de defensa frente a 72 ataques documentados y concluyeron que solo su

⁵ Vulnerability Exploitability eXchange: declaración del fabricante que indica si una vulnerabilidad presente en un componente afecta o no, de forma explotable, a un producto concreto.

⁶ Supply-chain Levels for Software Artifacts: marco de niveles para la integridad y procedencia de artefactos de compilación. <https://slsa.dev>

combinación ofrece una transparencia, pero no está cobertura adecuada; señalan, por ejemplo, que el SBOM aporta autenticado si no se acompaña de firmas y atestaciones.

Ilustración 2.

Controles técnicos para asegurar la cadena de suministro de software

Controles técnicos para asegurar la cadena de suministro de software

Qué responde cada control y en qué etapa actúa

Control	Pregunta que responde	Etapa principal
SSDF NIST SP 800-218	¿El proveedor desarrolla software con prácticas seguras verificables?	Proceso de desarrollo
SBOM SPDX · CycloneDX	¿Qué componentes y dependencias contiene el producto, y en qué versión?	Dependencias Consumidor
VEX	¿La vulnerabilidad de un componente es realmente explotable en este producto?	Consumidor Dependencias
SLSA Niveles de procedencia	¿El artefacto se compiló desde el código esperado, en un entorno aislado y trazable?	Compilación (CI/CD)
Sigstore Firma basada en identidad	¿Quién firmó el artefacto y está registrado en un log público de transparencia?	Repositorios y distribución
in-toto Atestaciones	¿Cada paso de la cadena lo ejecutó quien debía, en el orden definido?	Compilación Distribución

Propiedades de diseño seguro (Okafor et al., 2022)

Transparencia Visibilidad de componentes, pasos y actores (SBOM, logs)	Validez Integridad verificable de cada artefacto (firmas, procedencia)	Separación Aislamiento de etapas y privilegios mínimos en la cadena
--	--	---

Elaboración propia con base en Okafor et al. (2022), Newman et al. (2022), Abu Ishgair et al. (2024), NIST⁴ y SLSA⁶.

2.3. Nueva regulación: Cyber Resilience Act, NIS2 y el enfoque de Estados Unidos

En pocos años, la seguridad de la cadena de suministro de software pasó de ser una buena práctica voluntaria a convertirse en una obligación legal. La Unión Europea y Estados Unidos, sin embargo, han seguido caminos

distintos: la primera ha optado por obligaciones horizontales con sanciones y vigilancia de mercado, mientras que el segundo ha utilizado las compras públicas como palanca y, desde 2025, ha flexibilizado sus exigencias.

En Europa, la Directiva NIS2⁷, en vigor desde enero de 2023 y con plazo de transposición hasta octubre de 2024, obliga a las entidades esenciales e importantes a gestionar la seguridad de la cadena de suministro, incluidas sus relaciones con proveedores directos, y a considerar las vulnerabilidades y prácticas de desarrollo seguro de cada uno de ellos. NIS2 regula, por tanto, a quien usa el software; el CRA, en cambio, regula a quien lo fabrica.

El Cyber Resilience Act⁸, en vigor desde el 10 de diciembre de 2024, es la primera norma que impone requisitos horizontales de ciberseguridad a todos los productos con elementos digitales, de hardware o de software, que se comercialicen en la Unión Europea. Exige seguridad desde el diseño, la elaboración de un SBOM en formato legible por máquina, la gestión de vulnerabilidades

durante un periodo de soporte declarado y el marcado CE. Desde el 11 de septiembre de 2026, los fabricantes deben notificar las vulnerabilidades activamente explotadas y los incidentes graves a través de la plataforma única de ENISA, con una alerta temprana en 24 horas, una notificación en 72 horas y un informe final⁹; la aplicación plena llegará el 11 de diciembre de 2027.

Chiara (2025) caracteriza el CRA como una regulación de enfoque horizontal, basada en el riesgo y en la lógica de seguridad de productos, y advierte que, a diferencia de otras normas europeas, carece de mecanismos explícitos de protección de derechos fundamentales, además de generar incertidumbre jurídica en algunas de sus disposiciones de aplicación. Para el software libre, el reglamento crea la figura del «administrador de código abierto», con obligaciones reducidas y sin

⁷ Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo (NIS2). <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>

⁸ Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo, relativo a requisitos horizontales de ciberseguridad para los productos con

elementos digitales (Cyber Resilience Act). <https://eur-lex.europa.eu/eli/reg/2024/2847/oj>

⁹ Comisión Europea. Cyber Resilience Act – Reporting obligations. <https://digital-strategy.ec.europa.eu/en/policies/cra-reporting>

multas; Tridgell y Singh (2025) la consideran un modelo de gobernanza novedoso, pero alertan sobre el riesgo de que los acuerdos informales debiliten la equidad, la rendición de cuentas y la transparencia de las comunidades.

En Estados Unidos, la Orden Ejecutiva 14028 de 2021¹⁰ impulsó el SBOM y el marco SSDF, y el memorando OMB M-22-18 exigió a los proveedores del gobierno federal atestar sus prácticas de desarrollo seguro. La Orden Ejecutiva 14144 de enero de 2025 reforzó esas atestaciones, pero la Orden Ejecutiva 14306 de junio de 2025 eliminó dichos refuerzos, aunque mantuvo la actualización del SSDF¹¹. En 2026, el memorando OMB M-26-05 derogó M-22-18 y

dejó la atestación y el SBOM a criterio de cada agencia, según su evaluación de riesgos¹².

Para las organizaciones latinoamericanas, este panorama tiene implicaciones directas: el CRA se aplica a cualquier fabricante que comercialice productos en el mercado europeo, con independencia de su país de origen, por lo que las empresas de software de la región que exportan a Europa deben prepararse para cumplirlo. Al mismo tiempo, los controles descritos en este boletín pueden adoptarse de manera voluntaria como buena práctica, y la investigación académica sigue siendo necesaria para evaluar su efectividad real (Williams et al., 2025).

¹⁰ NIST. Executive Order 14028, Improving the Nation's Cybersecurity. <https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity>

¹¹ Davis Wright Tremaine (2025). Trump cyber order changes Biden EO 14144. <https://www.dwt.com/blogs/privacy-->

[security-law-blog/2025/06/trump-cyber-order-changes-biden-eo-14144](https://www.dwt.com/blogs/privacy--security-law-blog/2025/06/trump-cyber-order-changes-biden-eo-14144)

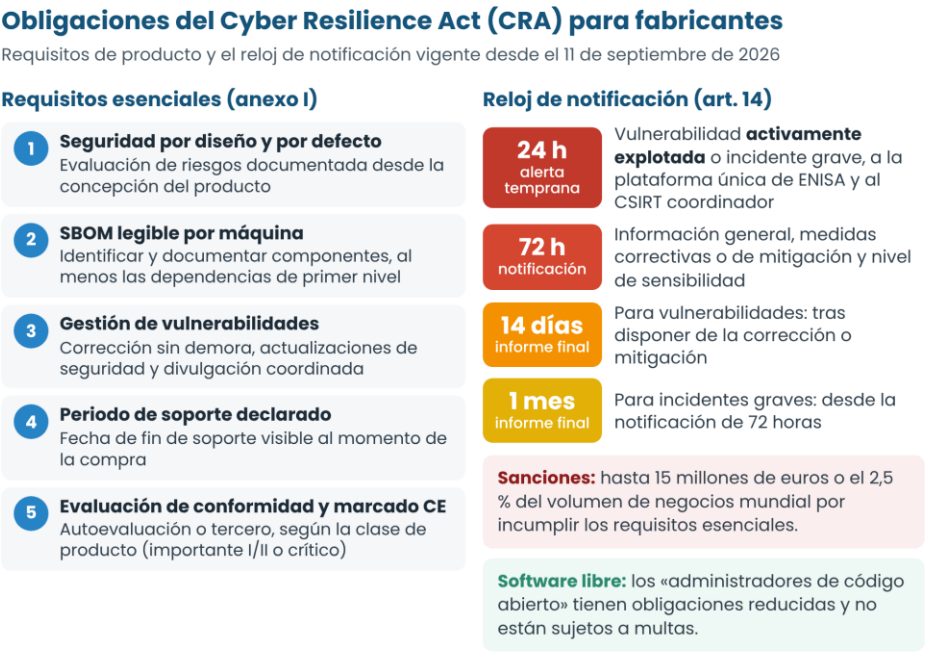
¹² Davis Wright Tremaine (2026). OMB changes course on software security. <https://www.dwt.com/blogs/privacy--security-law-blog/2026/02/omb-changes-course-on-software-security>

Ilustración 3.
Línea de tiempo de la nueva regulación sobre la cadena de suministro de software



Elaboración propia con base en EUR-Lex⁸, la Comisión Europea⁹, NIST¹⁰ y Davis Wright Tremaine¹².

Ilustración 4.
Obligaciones del Cyber Resilience Act para fabricantes



Elaboración propia con base en el Reglamento (UE) 2024/2847⁸ y la Comisión Europea⁹.

3. Conclusiones

Este boletín permite identificar consensos claros sobre el estado de la seguridad de la cadena de suministro de software. En primer lugar, los ataques ya no se dirigen solo al producto final, sino a cualquier eslabón de la cadena: el código fuente, las dependencias, la compilación, los repositorios o los canales de actualización. Casos como SolarWinds, XZ Utils y Shai-Hulud confirman que el atacante busca el punto de mayor confianza y menor control para maximizar su alcance.

En segundo lugar, existe un conjunto maduro de controles técnicos, como el SSDF, el SBOM, el VEX, la firma basada en identidad, los niveles SLSA y las atestaciones in-toto, pero su adopción y su calidad siguen siendo desiguales. La evidencia muestra SBOM incompletos, herramientas que discrepan entre sí y dificultades prácticas de implementación, lo que confirma que ningún control aislado es suficiente y que su valor depende de combinarlos.

En tercer lugar, la regulación ha dejado de ser una recomendación para convertirse en obligación, aunque con enfoques divergentes. La Unión Europea, con NIS2 y sobre todo con el CRA, impone requisitos vinculantes, plazos de notificación de 24 y 72 horas y sanciones significativas, mientras que Estados Unidos ha transitado desde la atestación obligatoria hacia un modelo flexible basado en el riesgo de cada agencia.

Finalmente, el nuevo marco normativo traslada la responsabilidad a los fabricantes y abre debates aún no resueltos sobre el papel de las comunidades de código abierto. Para las organizaciones de la región, en especial las que exportan software a Europa, el año 2026 marca el inicio de una etapa en la que conocer y documentar la cadena de suministro será tanto una exigencia de seguridad como una condición de acceso al mercado.

4. Recomendaciones

A partir de los hallazgos sintetizados en este boletín, se formulan las siguientes recomendaciones dirigidas a equipos de desarrollo, CSIRT, líderes de seguridad, áreas de compras y responsables de la toma de decisiones tecnológicas:

- Mantener un inventario actualizado del software y sus dependencias, y generar SBOM de forma automática en la canalización CI/CD¹³, validando su completitud antes de entregarlos o utilizarlos.
- Complementar el SBOM con declaraciones VEX y con fuentes de explotación activa para priorizar las vulnerabilidades que afectan realmente a cada producto.
- Proteger el proceso de compilación y publicación mediante firma de artefactos basada en identidad, verificación de procedencia según los niveles SLSA y autenticación multifactor en las cuentas de los repositorios.
- Establecer criterios de selección y monitoreo de dependencias de código abierto, considerando su mantenimiento, su historial de seguridad y la fijación de versiones verificadas.
- Incluir requisitos de seguridad de la cadena de suministro en los contratos con proveedores, como la alineación con el SSDF, la entrega de SBOM y los plazos de notificación de vulnerabilidades.
- Evaluar, en las organizaciones que comercializan productos en Europa, su exposición al CRA y preparar desde ahora los procesos de notificación en 24 y 72 horas, el periodo de soporte y la documentación técnica exigida.
- Promover, desde la academia y los CSIRT, la formación en seguridad de la cadena de suministro y la investigación sobre la efectividad de estos controles en el contexto latinoamericano.

¹³ Integración Continua y Entrega/Despliegue Continuo.

5. Referentes Bibliográficos

- Abu Ishgair, E., Melara, M. S., & Torres-Arias, S. (2024). SoK: A defense-oriented evaluation of software supply chain security (Versión 1). arXiv. <https://doi.org/10.48550/arXiv.2405.14993>
- Balliu, M., Baudry, B., Bobadilla, S., Ekstedt, M., Monperrus, M., Ron, J., Sharma, A., Skoglund, G., Soto-Valero, C., & Wittlinger, M. (2023). Challenges of producing software bill of materials for Java. *IEEE Security & Privacy*, 21(6), 12–23. <https://doi.org/10.1109/MSEC.2023.3302956>
- Chiara, P. G. (2025). Understanding the regulatory approach of the Cyber Resilience Act: Protection of fundamental rights in disguise? *European Journal of Risk Regulation*, 16(2), 469–484. <https://doi.org/10.1017/err.2025.9>
- Enck, W., & Williams, L. (2022). Top five challenges in software supply chain security: Observations from 30 industry and government organizations. *IEEE Security & Privacy*, 20(2), 96–100. <https://doi.org/10.1109/MSEC.2022.3142338>
- Ladisa, P., Plate, H., Martinez, M., & Barais, O. (2023). SoK: Taxonomy of attacks on open-source software supply chains. En 2023 *IEEE Symposium on Security and Privacy (SP)* (pp. 1509–1526). IEEE. <https://doi.org/10.1109/SP46215.2023.10179304>

Martínez, J., & Durán, J. M. (2021). Software supply chain attacks, a threat to global cybersecurity: SolarWinds' case study. *International Journal of Safety and Security Engineering*, 11(5), 537–545.

<https://doi.org/10.18280/ijssse.110505>

Newman, Z., Meyers, J. S., & Torres-Arias, S. (2022). Sigstore: Software signing for everybody. En *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* (pp. 2353–2367). ACM.

<https://doi.org/10.1145/3548606.3560596>

O'Donoghue, E., Hastings, Y., Ortiz, E., & Manzi Muneza, A. R. (2025). *Software bill of materials in software supply chain security: A systematic literature review* (Versión 1). arXiv.

<https://doi.org/10.48550/arXiv.2506.03507>

Ohm, M., Plate, H., Sykosch, A., & Meier, M. (2020). Backstabber's knife collection: A review of open source software supply chain attacks. En *Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA 2020)* (pp. 23–43). Springer. https://doi.org/10.1007/978-3-030-52683-2_2

Okafor, C., Schorlemmer, T. R., Torres-Arias, S., & Davis, J. C. (2022). SoK: Analysis of software supply chain security by establishing secure design properties. En *Proceedings of the 2022 ACM Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses (SCORED '22)*. ACM. <https://doi.org/10.1145/3560835.3564556>

Stalnaker, T., Wintersgill, N., Chaparro, O., Di Penta, M., German, D. M., & Poshyvanyk, D. (2024). BOMs away! Inside the minds of stakeholders: A comprehensive study of bills of materials for software systems. En *Proceedings of the IEEE/ACM 46th International Conference on Software Engineering (ICSE '24)* (pp. 1–13). ACM.

<https://doi.org/10.1145/3597503.3623347>

Tridgell, J., & Singh, J. (2025). 'Stewardship' as a fair, accountable and transparent model for free and open-source software governance? Looking beyond the EU's Cyber Resilience Act. En *Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency (FAccT '25)* (pp. 454–465). ACM.

<https://doi.org/10.1145/3715275.3732032>

Williams, L., Benedetti, G., Hamer, S., Paramitha, R., Rahman, I., Tamanna, M., Tystahl, G., Zahan, N., Morrison, P., Acar, Y., Cukier, M., Kästner, C., Kapravelos, A., Wermke, D., & Enck, W. (2025). Research directions in software supply chain security. *ACM Transactions on Software Engineering and Methodology*, 34(5), 1–38.

<https://doi.org/10.1145/3714464>

Xia, B., Bi, T., Xing, Z., Lu, Q., & Zhu, L. (2023). An empirical study on software bill of materials: Where we stand and the road ahead. En *2023 IEEE/ACM 45th International Conference on Software Engineering*

(ICSE) (pp. 2630–2642). IEEE.

<https://doi.org/10.1109/ICSE48619.2023.00219>

Zahan, N., Lin, E., Tamanna, M., Enck, W., & Williams, L. (2023). Software bills of materials are required. Are we there yet? *IEEE Security & Privacy*, 21(2), 82–88. <https://doi.org/10.1109/MSEC.2023.3237100>