ESTUDIO DE CIBERSEGURIDAD EN LA CADENA DE SUMINISTRO

Resiliencia como Propiedad Colectiva del Ecosistema Logístico

Centro Español de Logística (CEL)
Zaragoza Logistics Center (ZLC)

2026

Patrocinado por:

ÍNDICE

Bienvenida 3
Equipo de trabajo 6
1. Resumen ejecutivo 7
2. Introducción 8
2.1. Objetivo y alcance 8
2.2. Metodología 9
2.3. Glosario de términos 10
3. Contexto actual de las cadenas de suministro 11
3.1. Globalización de las cadenas logísticas 11
3.2. Situación geopolítica 11
3.3. Digitalización 12
3.4. Evolución tecnológica de la cadena de suministro 12
3.5. Magnitud del riesgo: datos globales 13
4. La ciberseguridad como principal amenaza de las cadenas de suministro 14
4.1. Normativa actual 15
4.2. Riesgos, amenazas e impacto (económico, operativo y social) 16
4.3. Ecosistema de proveedores y clientes 17
4.4. Principales vulnerabilidades 19
4.5. Prevención, monitorización y planes de contingencia para cadenas de suministro resilientes .. 22
4.6. Tecnologías que habilitan la resiliencia 23
5. Análisis de la encuesta de ciberseguridad en las cadenas de suministro 25
5.1. Perfil de la muestra 25
5.2. Estrategia y percepción del riesgo 26
5.3. Cultura organizativa y factor humano 27
5.4. Amenazas e inteligencia artificial 28
5.5. Madurez en la implementación de medidas 29
5.6. Gestión del riesgo de proveedores 30
5.7. Impacto potencial: continuidad y resiliencia financiera 31
6. Desafíos y oportunidades de futuro 33
7. Conclusiones finales 35
8. Decálogo 37
9. Bibliografía 40

BIENVENIDA



Ramón García

Director General del Centro Español de Logística

El riesgo no termina en nuestra organización.

Una cadena de suministro no se mueve únicamente con mercancías, se mueve también con información. Detrás de cada previsión, pedido, inventario, ruta, proceso productivo o entrega hay datos que circulan entre organizaciones, sistemas y personas. Esa conexión permanente ha permitido operar con más visibilidad, coordinación y eficiencia, pero también ha creado nuevas dependencias y una superficie de exposición cada vez mayor.

La ciberseguridad ocupa, por ello, un lugar cada vez más relevante en la gestión logística. Una incidencia tecnológica puede afectar a un almacén, bloquear una expedición, alterar un aprovisionamiento o comprometer información crítica. Y, en un entorno tan interconectado, el origen del problema puede estar muy lejos del punto en el que finalmente se manifiestan sus consecuencias.

La preparación depende de conocer esas relaciones, identificar qué procesos y actores son realmente críticos y establecer mecanismos que permitan prevenir, detectar, responder y recuperar la operativa. También depende de las personas. En logística, donde la información atraviesa constantemente distintos equipos y organizaciones, la cultura de seguridad forma parte de la manera en que trabajamos y tomamos decisiones.

Esta preocupación no es nueva para CEL, hace años ya abordamos estas cuestiones en nuestra Guía de Seguridad de la Información en la Cadena de Suministro y en las Infraestructuras Críticas, cuando la ciberseguridad todavía no ocupaba el espacio que hoy tiene en la agenda empresarial. Entonces señalábamos la necesidad de proteger no solo los sistemas, sino también la información, las infraestructuras y las relaciones que sostienen la actividad logística. La evolución de las cadenas de suministro ha reforzado aquella visión y ha hecho el desafío mucho más complejo.

Ese recorrido encuentra ahora continuidad en el Estudio de Ciberseguridad en la Cadena de Suministro. Resiliencia como Propiedad Colectiva del Ecosistema Logístico, desarrollado conjuntamente por GMV, ZLC y CEL. Esta colaboración nos permite reunir conocimiento y perspectivas complementarias para analizar la ciberseguridad desde la realidad de las empresas con actividad logística y desde las decisiones que deben afrontar sus profesionales.

El estudio parte de una idea esencial, la resiliencia de una cadena no puede construirse de forma individual. La capacidad de respuesta de cada organización está condicionada por la preparación de quienes forman parte de su ecosistema; y gestionar esas dependencias implica incorporar la ciberseguridad a la relación con proveedores y colaboradores, a la continuidad de negocio, a la formación de los equipos y a las decisiones estratégicas.

Hemos querido que este trabajo vaya más allá del análisis y resulte útil para la acción. Además de ofrecer una visión de la situación actual, busca ayudar a establecer prioridades y avanzar de manera ordenada hacia cadenas de suministro más resilientes. El decálogo de buenas prácticas que acompaña sus conclusiones responde a esa misma voluntad, traducir el conocimiento en criterios aplicables y, al mismo tiempo, contribuir a sensibilizar sobre una responsabilidad que es necesariamente compartida.

En el CEL entendemos que generar conocimiento significa identificar los cambios que están transformando la logística, analizarlos con rigor y convertir ese análisis en herramientas que puedan ser utilizadas por las empresas. Ese trabajo de observación y anticipación nos permite acompañar la evolución de la actividad logística y poner el conocimiento al servicio de los retos que van surgiendo. Esa labor está estrechamente unida a otra de nuestras responsabilidades, contribuir a desarrollar profesionales preparados para afrontar esos cambios, con conocimientos y capacidades ajustados a las necesidades reales de las organizaciones.

La digitalización seguirá aumentando la interdependencia de nuestras cadenas de suministro. Afrontar esa realidad exige más preparación, más conocimiento y una mayor coordinación entre organizaciones. Este estudio quiere contribuir a ese camino, porque la ciberresiliencia se construye necesariamente entre todos los eslabones de la cadena.



Carolina Ciprés

Directora de Investigación de Zaragoza Logistics Center (ZLC)

Ciberseguridad y resiliencia: desafíos para las cadenas de suministro del futuro.

En los últimos años, la seguridad de las cadenas de suministro ha pasado de ser un asunto operativo a una cuestión estratégica. En un contexto marcado por tensiones geopolíticas, fenómenos climáticos extremos, envejecimiento de infraestructuras críticas y un incremento constante de los ciberataques, las organizaciones necesitan replantearse cómo gestionar los riesgos y fortalecer su capacidad de adaptación ante la incertidumbre.

Este estudio conjunto de CEL y ZLC muestra que la ciberseguridad no puede analizarse de forma aislada, sino como parte de un enfoque integral de resiliencia de la cadena de suministro. Ya no se trata solo de cómo proteger los sistemas de información frente a ciberataques. El verdadero reto consiste en construir cadenas capaces de mantener su funcionamiento cuando convergen amenazas digitales, físicas e híbridas. La resiliencia requiere desarrollar capacidades de anticipación, respuesta y transformación que permitan minimizar el impacto de las disrupciones y garantizar la continuidad de las operaciones.

Tradicionalmente, la seguridad física y la ciberseguridad se han abordado como disciplinas independientes. Sin embargo, la creciente digitalización de la logística está difuminando esta frontera. Un incidente cibernético puede comprometer la operativa de infraestructuras críticas, afectar la planificación del transporte o reducir la visibilidad de los flujos logísticos. Del mismo modo, una interrupción física puede generar vulnerabilidades que incrementen el riesgo digital. Esta convergencia de amenazas exige enfoques integrados para comprender y gestionar los riesgos de manera coordinada.

Zaragoza Logistics Center desarrolla desde hace años líneas de investigación centradas en el fortalecimiento de la resiliencia de la cadena de suministro, aplicando metodologías de análisis de riesgos y herramientas de apoyo a la toma de decisiones. En este ámbito, iniciativas europeas como RISE-SME han analizado cómo las pequeñas y medianas empresas pueden reforzar su resiliencia a través de la adopción de tecnologías digitales.

Más recientemente, el proyecto europeo TRANSCEND ha ampliado este enfoque al ámbito del transporte de mercancías, abordando de manera conjunta amenazas físicas, digitales e híbridas. El proyecto permite avanzar desde una gestión reactiva hacia una gestión proactiva del riesgo, mejorando la capacidad de anticipación y respuesta en las redes de transporte.

Los próximos años estarán marcados por una creciente incorporación de inteligencia artificial, sensores avanzados y robotización. Estas tecnologías ofrecerán nuevas oportunidades para mejorar la eficiencia, la visibilidad y la capacidad predictiva de las cadenas de suministro, pero también aumentarán la vulnerabilidad ante ciberamenazas. En consecuencia, la ciberseguridad deberá integrarse plenamente en las estrategias de transformación digital.

Este estudio muestra que la tecnología es una condición necesaria para mejorar la ciberseguridad, pero no suficiente. Las cadenas de suministro resilientes serán, en gran medida, el resultado de la calidad de las decisiones que tomen las personas que las gestionan. En un contexto de creciente complejidad e incertidumbre, el talento será el factor diferencial para construir cadenas de suministro más seguras, adaptables y fiables.



Mariano J. Benito

Cybersecurity & Privacy Ambassador de GMV

La digitalización está transformando profundamente la actividad logística.

La eficiencia operativa y la capacidad de servicio se ven impulsadas por sistemas IT como plataformas de gestión del transporte, almacenes automatizados, dispositivos IoT, soluciones de seguimiento en tiempo real o servicios en la nube. Muchos de estos sistemas y servicios IT están accesibles para los operadores logísticos o sus empleados desde cualquier ubicación. Sin embargo, esta mayor conectividad amplía de forma inevitable la superficie de exposición frente a ciberamenazas externas. Y, en consecuencia, aumentan los riesgos de ciberseguridad. El resultado es claro: organizaciones más eficientes y ágiles, pero también más vulnerables.

Este fenómeno es común a todos los sectores económicos, incluido el logístico. El World Economic Forum ya identifica en los últimos años la ciberseguridad como uno de los principales riesgos globales, mientras que ENISA, en su informe "Threat Landscape 2025", destaca amenazas como el phishing, el ransomware, los ataques a dispositivos móviles y los riesgos derivados de la cadena de suministro, tanto de los proveedores directos como de sus proveedores.

En estos momentos, la actividad logística tiene dos misiones. Debe proteger sus propias operaciones, y también debe garantizar la continuidad de negocio de sus clientes en otros sectores. Esta doble misión la convierte en un objetivo prioritario para los ciberdelincuentes, como en el uso fraudulento de marcas logísticas en campañas de phishing. También las empresas logísticas han sufrido ciberincidentes y han generado incidentes de ciberseguridad a sus clientes.

Este escenario demanda tomar decisiones activamente. La ciberseguridad y la ciberresiliencia deben integrarse en la cultura y la estrategia empresarial. Esto implica incorporar la gestión de riesgos de ciberseguridad en la toma de decisiones, reforzar las capacidades de prevención, detección y respuesta, y extender la concienciación a todos los niveles de la organización, desde operaciones hasta la alta dirección. Y contar con soluciones y proveedores especializados y comprometidos con la seguridad de todos los sectores.

Además, el marco regulatorio europeo, con iniciativas como NIS2, CER o el Cybersecurity Act, actuará como catalizador para acelerar la integración de ciberseguridad y la ciberresiliencia, elevando el nivel de seguridad que aplican los operadores logísticos.

Desde GMV, confiamos en que este estudio contribuya a visibilizar los principales retos del sector y a impulsar una cultura de ciberseguridad y ciberresiliencia sólida que proteja a empresas y clientes de logística.

EQUIPO DE TRABAJO

Equipo técnico



Gisèle Muñoz
Directora de Innovación y Desarrollo



Sonia Ramudo
Responsable de Proyectos

Comunicación



Marina Cisneros
Responsable de Comunicación y Relaciones Institucionales

Equipo técnico



Susana Val
Profesora Asociada de Investigación y Subdirectora del Instituto de Investigación Adscrito ZLC



Tamara Pardo
Técnica de Oficina de Investigación

Comunicación



Sira Marqueta
Directora de Marketing



Sonia Román
Marketing Lead

1. RESUMEN EJECUTIVO

La digitalización acelerada propia de la Industria 4.0 y 5.0 ha multiplicado la interconectividad entre sistemas mediante el Internet de las Cosas (IoT) y el Internet de los Servicios (IoS). Esta interdependencia genera eficiencias notables, pero también expone a las organizaciones a **vulnerabilidades** cada vez más sofisticadas que afectan directamente a sus **cadenas de suministro**.

En un mercado globalizado y altamente distribuido, los **ciberataques** ya no se dirigen únicamente al objetivo final: Se apoyan en proveedores con menores capacidades de protección para penetrar en ecosistemas completos. La opacidad de los niveles superiores de la cadena, sumada a la heterogeneidad de prácticas de seguridad entre actores, ha consolidado los ataques a proveedores como uno de los vectores más críticos de la amenaza digital contemporánea.

La ciberseguridad en las cadenas de suministro ha dejado de ser un asunto técnico marginal para convertirse en un elemento central de la continuidad de negocio en un entorno económico cada vez más interconectado y geopolíticamente incierto.

El presente estudio examina el **estado del arte en ciberseguridad aplicada a las cadenas de suministro**, revisa **marcos tecnológicos y regulatorios** emergentes y propone una visión sistémica basada en la **resiliencia como propiedad colectiva del ecosistema logístico**. Integra evidencia empírica reciente procedente de revistas académicas de alto impacto, informes institucionales de organismos, y datos de incidentes reales acaecidos entre 2024 y 2026.

39%

de los expertos identifican los ciberataques como el 5º riesgo global más relevante[1]

61%

de crecimiento en ciberataques a transportistas y proveedores logísticos durante 2025[2]

60%

de las brechas de seguridad tienen al factor humano como elemento presente[3]

42 días

es el tiempo medio de permanencia de un atacante en entornos industriales de Operational Technology (OT) antes de ser detectado[4]

Palabras clave: Ciberseguridad · Cadena de suministro · Resiliencia · Industria 4.0 · Gestión del riesgo cibernético · NIS2 · Pyme · Factor humano

[1] World Economic Forum. (2024). The global risks report 2024. WEF. https://www.weforum.org/reports/global-risks-report-2024/
[2] Everstream Analytics. (2026). Supply chain risk report 2026. https://www.everstream.ai/special-reports/2026-annual-supply-chain-risk-report/
[3] Verizon Business. (2025). 2025 Data Breach Investigations Report (DBIR). Verizon. https://www.verizon.com/business/resources/reports/dbir/
[4] Dragos. (2026). 2026 OT/ICS cybersecurity year in review. Dragos, Inc. https://www.dragos.com/ot-cybersecurity-year-in-review

2. INTRODUCCIÓN

2.1. Objetivo y alcance

El presente estudio tiene como objetivo analizar el **estado actual de la ciberseguridad en las cadenas de suministro en España**, identificar las **principales amenazas y vulnerabilidades**, y proporcionar a los profesionales del sector **un marco de referencia práctico para mejorar su resiliencia frente a los riesgos cibernéticos**.

El destinatario prioritario es el profesional de la logística y la cadena de suministro que necesita comprender el paisaje del riesgo cibernético y disponer de criterios de acción concretos, independientemente del tamaño de su organización. El estudio es igualmente relevante para responsables de tecnología, directores de operaciones, responsables de compras y directivos con responsabilidad sobre la continuidad del negocio.

El alcance del análisis abarca tanto las dimensiones técnicas como organizativas y regulatorias de la ciberseguridad en la cadena de suministro, con especial atención a la realidad del tejido empresarial español, mayoritariamente compuesto por pymes.



Objetivo

Analizar y comprender el **estado actual de la ciberseguridad** en la cadena de suministro en España.

Alcance

Desde las **dimensiones técnicas y organizativas** hasta el **marco regulativo** y el impacto en el tejido empresarial.

Enfoque

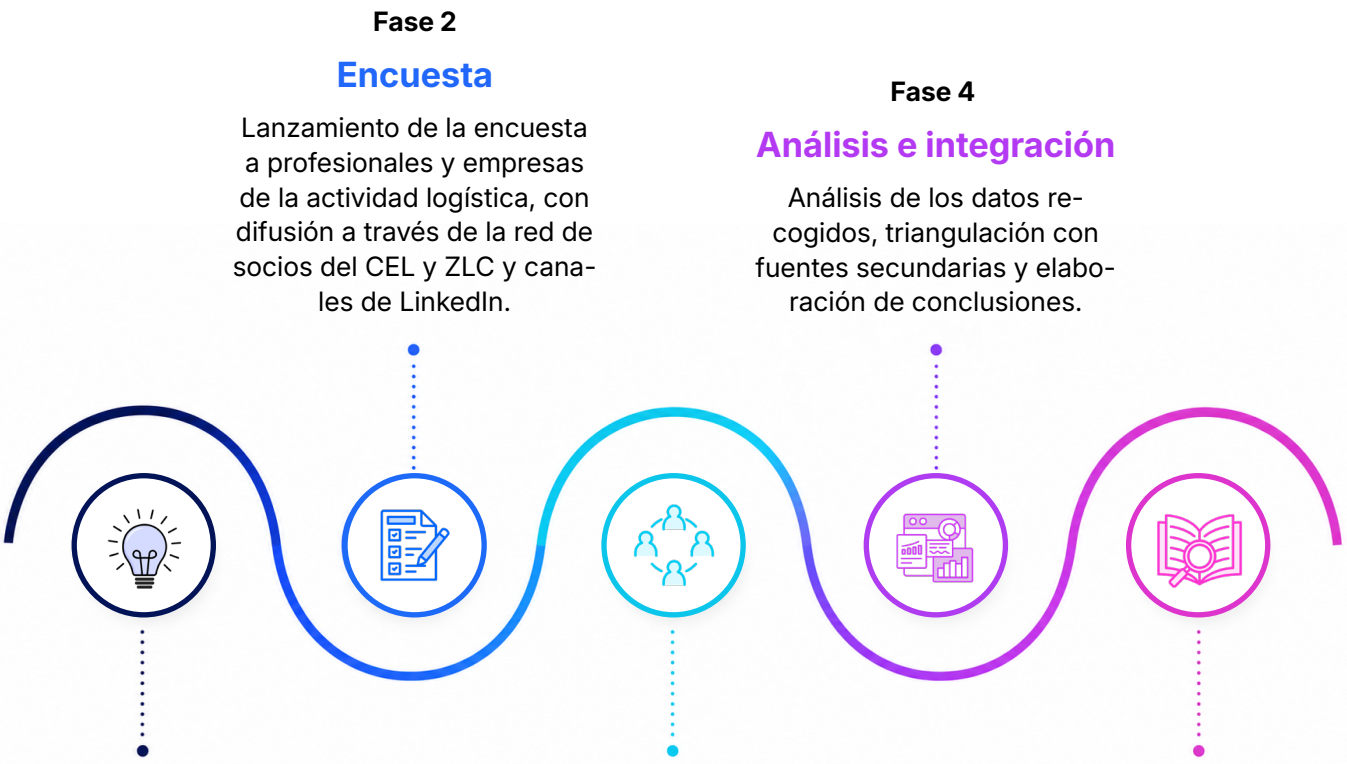
Práctico y aplicado, con especial atención a la **realidad del mercado español** y a las **pymes**.

2.2. Metodología

Este estudio combina una **revisión** sistemática del **estado del arte** académico e institucional en **ciberseguridad** aplicada a cadenas de suministro con un **análisis cuantitativo y cualitativo** basado en datos primarios recogidos mediante **encuesta** y **grupos de trabajo** con profesionales de la actividad logística española.

La revisión bibliográfica integra evidencia empírica procedente de revistas académicas de alto impacto (Journal of Operations Management, Supply Chain Management: An International Journal, International Journal of Production Research, entre otras), informes institucionales de organismos de referencia (ENISA, IBM, Verizon, Everstream Analytics, WEF, NIST) y datos de incidentes reales acaecidos entre 2024 y 2026.

El trabajo de campo se estructura en las siguientes fases:



2.3. Glosario de términos

BIA (Business Impact Analysis)

Análisis de Impacto de Negocio. Metodología que identifica procesos críticos y cuantifica el impacto de distintos escenarios de disrupción.

Cadena de suministro

Conjunto de actividades, procesos y agentes que participan en el **flujo de bienes y servicios** desde el origen hasta el consumidor final.

Cibercadena de suministro

Ecosistema digital que **soporta y conecta todos los procesos logísticos**, integrando flujos digitales, plataformas de datos, software, sensores, APIs y sistemas interconectados.

Ciberresiliencia

Capacidad de una organización para **anticipar, absorber, adaptarse** y recuperarse de un **incidente de ciberseguridad** manteniendo la continuidad operativa.

Convergencia IT/OT

Integración de las **Tecnologías de la Información** (sistemas corporativos) con las **Tecnologías de Operación** (sistemas de control industrial), generando nuevas superficies de ataque.

Deepfakes

Contenidos audiovisuales (audio, vídeo o imagen) generados o **manipulados** mediante técnicas de inteligencia artificial que permiten **suplantar** de forma realista la **identidad de personas**, con fines potenciales de desinformación, fraude o ingeniería social.

NIS2

Directiva europea de **Seguridad de Redes y Sistemas de Información**, que amplía las obligaciones de ciberseguridad a 18 sectores críticos y refuerza los controles sobre proveedores.

Phishing

Técnica de ciberataque basada en el **envío masivo de comunicaciones** fraudulentas (normalmente correos electrónicos o mensajes) que simulan provenir de fuentes legítimas con el objetivo de engañar al destinatario para que revele información sensible o realice acciones maliciosas.

Pyme

Pequeña y mediana empresa, que en España y Europa constituye el grueso del tejido empresarial logístico.

Ransomware

Tipo de malware que cifra los activos digitales de la víctima y **exige un rescate** económico para restablecer el acceso.

SOC (Security Operations Center)

Centro de operaciones de seguridad que proporciona monitorización y detección de amenazas de forma continua (24/7).

Spear phishing

Variante avanzada y dirigida del phishing en la que el **ataque se personaliza** para una persona, organización o rol específico, utilizando información contextual previa para aumentar su credibilidad y probabilidad de éxito.

Zero Trust Architecture (ZTA)

Modelo de seguridad que elimina la confianza implícita y **exige verificación** continua para usuarios, dispositivos y sistemas, con el principio rector de «nunca confiar, siempre verificar».

3. CONTEXTO ACTUAL DE LAS CADENAS DE SUMINISTRO

3.1. Globalización de las cadenas logísticas

La **cadena de suministro** contemporánea funciona como un **sistema global articulado** por **proveedores** distribuidos en **múltiples niveles y geografías**. Esta arquitectura multicapa ofrece eficiencia, escalabilidad y optimización, pero también genera zonas en las que la visibilidad disminuye significativamente a medida que las empresas se alejan de sus proveedores de nivel directo.

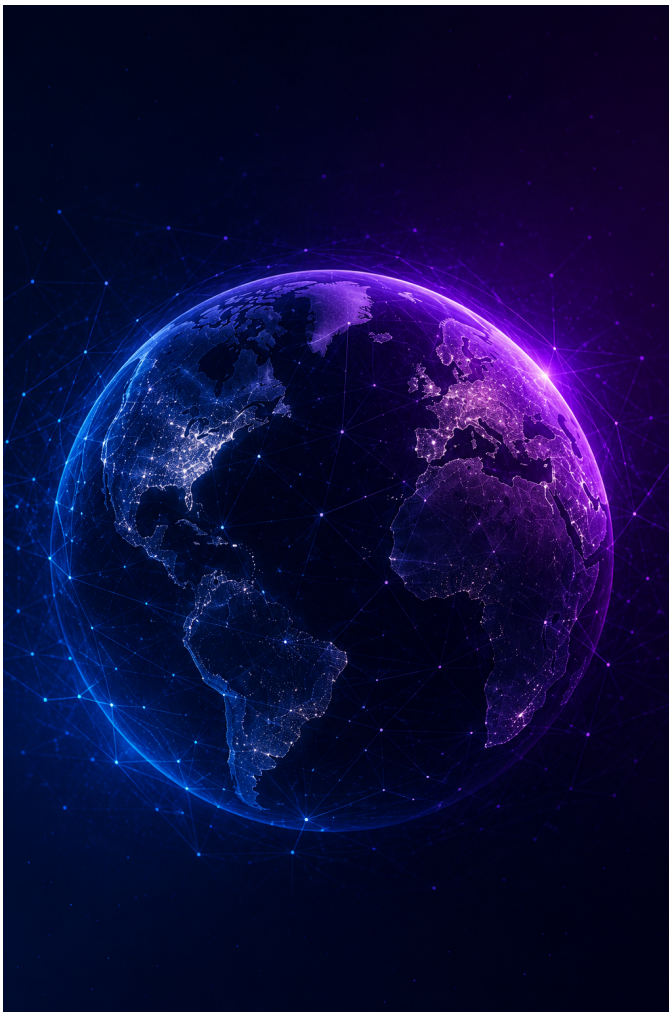
La deslocalización intensiva del período 2005-2008 incrementó la complejidad geográfica generando mayor dependencia de proveedores globales con visibilidad muy reducida más allá del proveedor de primer nivel. Esta falta de visibilidad en la cadena de suministro agravó los efectos de la crisis de 2009-2012, y el mismo patrón se repitió durante la pandemia de COVID-19, cuando las organizaciones necesitaron sistemas predictivos, visibilidad de extremo a extremo y capacidad de reacción ante cambios súbitos.

La **globalización** de las cadenas también genera **interdependencias** que amplifican el impacto de cualquier disrupción: La caída de un único proveedor tecnológico o logístico puede propagarse de forma inmediata a todo el ecosistema de organizaciones que dependen de él.

3.2. Situación geopolítica

El escenario internacional de 2025-2026 actúa como catalizador de un cambio de era marcado por la erosión del orden multilateral de posguerra y la transición hacia un sistema fragmentado donde predomina la lógica de la fuerza. En este **entorno altamente volátil**, la inestabilidad política, los conflictos armados y el debilitamiento de las instituciones globales generan condiciones ideales para un aumento exponencial de las denominadas **amenazas híbridas**.

> *La fragmentación geopolítica se sitúa con un nivel de amenaza del 97% para las cadenas de suministro globales, identificándola como el riesgo más significativo del año.*
>
> **Informe de riesgo de Everstream Analytics 2026**[2]



En Europa, la **incertidumbre geopolítica** ha aumentado debido a la menor estabilidad en la relación transatlántica, el auge de movimientos populistas y el impacto prolongado de la guerra en Ucrania y la presión estratégica de Rusia. Los ataques de guerra híbrida, incluyendo interferencias GPS y bloqueos de comunicaciones en el Báltico, interrumpen el tráfico aéreo y marítimo, con un crecimiento del 61% en ciberataques a transportistas y proveedores logísticos durante 2025[2].

En Oriente Próximo, la inestabilidad estructural de la región ha alcanzado en 2026 una nueva fase crítica. El colapso de regímenes, la operación militar sobre Irán y el cierre del estrecho de Ormuz, por el que transita aproximadamente el 20% del comercio mundial de petróleo, han generado una crisis energética y logística de primer orden. En este entorno, actores estatales y no estatales recurren a métodos asimétricos, incluidos los ciberataques, para compensar debilidades militares convencionales o presionar a rivales.

De esta forma, el entorno geopolítico actual impulsa el incremento sostenido de los ciberataques en la cadena de suministro. Las organizaciones ya no pueden tratar la ciberseguridad como una cuestión técnica interna; es una dimensión de su estrategia competitiva en un orden global marcado por la coerción.

3.3. Digitalización

La **digitalización de la cadena de suministro** ha seguido un proceso gradual pero acelerado. Entre 2013 y 2017, la adopción de sistemas ERP, EDI e interfaces estandarizadas marcó el inicio de la transición hacia modelos parcialmente digitalizados. A partir de 2017, surgieron arquitecturas logísticas basadas en IoT, Big Data y conectividad avanzada que permitieron monitorización continua e integración de flujos.

Esta transformación digital genera enormes oportunidades, pero también expande la superficie de ataque de manera exponencial. Cada nuevo sistema conectado, cada API, cada dispositivo IoT, es un potencial punto de entrada para un atacante.



3.4. Evolución tecnológica de la cadena de suministro

Los **pilares tecnológicos** actuales de la Supply Chain 4.0 incluyen el IoT y la tecnología RFID (Radio Frequency IDentification) para monitorización continua y granular; la analítica avanzada e **inteligencia artificial** para predicción de demanda y detección de anomalías; y los gemelos digitales para simulación de escenarios de riesgo y optimización de procesos antes de su ejecución real.

El informe de Everstream Analytics 2026[2] confirma que las organizaciones con mayor madurez digital presentaron una recuperación significativamente más rápida ante las disrupciones logísticas del período 2024-2026. Esta convergencia tecnológica crea simultáneamente nuevas superficies de ataque que requieren enfoques de ciberseguridad igualmente evolucionados.

3.5. Magnitud del riesgo: datos globales

Según el Informe de Riesgos Globales 2024 del Foro Económico Mundial[1], los ciberataques se posicionan como el quinto riesgo global más citado por los expertos, con un nivel de preocupación del 39%. Dentro de la categoría de riesgos tecnológicos, la desinformación generada por inteligencia artificial ha escalado hasta la segunda posición, siendo identificada por el 53% de los encuestados como amenaza crítica.

39%

de los expertos del World Economic Forum (WEF) identifican los ciberataques como uno de los cinco riesgos globales más críticos[1]

97%

nivel de amenaza de la fragmentación geopolítica para las cadenas de suministro[2]

61%

de crecimiento en ciberataques a transportistas logísticos durante 2025[2]

605

incidentes significativos registrados en España solo en el segundo semestre de 2025[5]

"El reto principal es la concienciación de la alta dirección. La ciberdelincuencia es ya la tercera economía mundial, solo por detrás de EE.UU. y China."

IT Head, empresa de logística y distribución.



[5] NTT DATA. (2026, febrero 16). España sufre tres ciberataques graves al día, con la industria en el punto de mira de los criminales. https://es.nttdata.com/news-folder/espana-ciberataques-industria-en-riesgo-2025

4. LA CIBERSEGURIDAD COMO PRINCIPAL AMENAZA DE LAS CADENAS DE SUMINISTRO

A medida que las empresas han reforzado su ciberseguridad interna, los atacantes han trasladado su foco hacia los **proveedores**. Los ataques a la cadena de suministro explotan la **debilidad** relativa de un **eslabón** para infiltrarse en toda una red. La complejidad de las cadenas actuales dificulta que una organización pueda auditar o supervisar a los actores más allá del primer nivel, y los atacantes lo saben: **Comprometer un proveedor secundario permite entrar en ecosistemas enteros de clientes de forma silenciosa y persistente**.

> *"Hay que hacer las cosas por convencimiento, no por cumplimiento. El cumplir y mentir no protege a nadie."*
>
> **Director de Supply Chain y Sostenibilidad, multinacional alimentaria.**



4.1. Normativa actual

Europa ha avanzado de forma decisiva para reforzar la resiliencia de las cadenas de suministro frente a las ciberamenazas mediante un conjunto de iniciativas regulatorias complementarias y estándares internacionales que configuran el marco de referencia en 2026:

Directiva NIS2

Amplía el alcance de las obligaciones en materia de ciberseguridad a 18 sectores considerados críticos, incluidos los sectores de Transporte, Energía y Fabricación, fortaleciendo los requisitos aplicables a la cadena de suministro y acortando los plazos para la notificación de incidentes. Su transposición en España convertirá la seguridad de la cadena de suministro en una obligación legal con consecuencias sancionadoras de hasta el 2% de la facturación anual global.

Cyber Resilience Act (CRA)

Aplica nuevas responsabilidades a los fabricantes de productos digitales, obligándoles a demostrar que sus dispositivos y software son seguros a lo largo de todo su ciclo de vida.

ISO/IEC 27036

Estándar internacional que ofrece pautas detalladas para gestionar la seguridad en las relaciones con proveedores, facilitando la evaluación y selección basada en criterios de ciberseguridad verificables.

ISO/IEC 27001:2022

Estándar internacional de referencia para el establecimiento, implementación y mejora continua de un sistema de gestión de seguridad de la información.

ISA/IEC 62443

Estándar de referencia global para la protección de entornos OT e ICS, incluyendo los sistemas SCADA, PLC y redes de automatización presentes en plantas logísticas y almacenes automatizados.

NIST SP 800-161r1

Guía que establece prácticas coherentes para la gestión del riesgo cibernético en la cadena de suministro, incluyendo un marco de cinco funciones: Identificar, proteger, detectar, responder y recuperar.

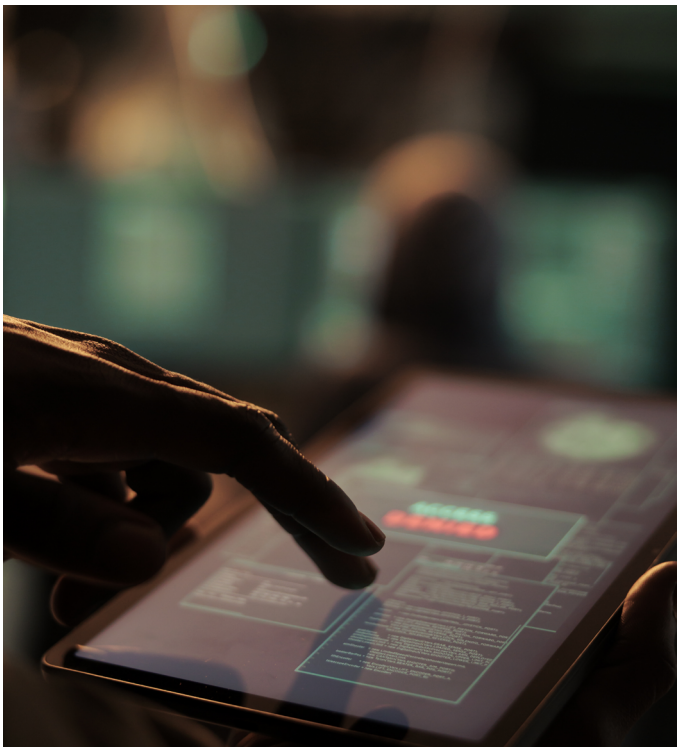
Esquema Nacional de Seguridad

Marco normativo español de obligado cumplimiento para el sector público y sus proveedores, certificable en categorías Básica, Media y Alta.

La actividad logística considera que el marco regulatorio está bien definido, pero su aplicación es desigual y su efectividad limitada. La percepción es que muchas organizaciones se centran en cumplir con el mínimo exigido, generando una sensación de seguridad más formal que real.

La falta de coordinación entre normativas -con diferentes calendarios y requisitos- y la heterogeneidad en la transposición de directivas europeas complican su implementación, especialmente en entornos internacionales.

Pese a ello, la actividad reconoce que la regulación ha aportado valor al establecer un nivel mínimo de referencia en ciberseguridad, inexistente en muchos casos anteriormente.



4.2. Riesgos, amenazas e impacto (económico, operativo y social)

Los riesgos cibernéticos en la cadena de suministro tienen un impacto tridimensional que va más allá de la pérdida económica directa:



Impacto operativo

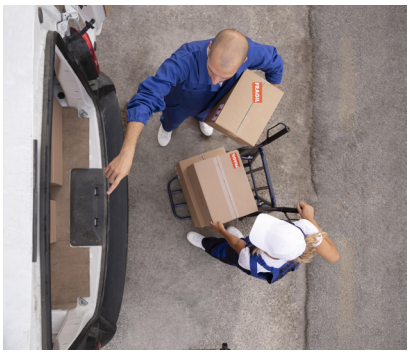
La **paralización de sistemas críticos** puede interrumpir la cadena de producción y distribución durante **días o semanas**. El sector industrial concentró más de dos tercios de las víctimas de ransomware en 2025[4], con un tiempo medio de permanencia del atacante de **42 días** antes de ser detectado.

De hecho, se constata que los ataques de ransomware pueden paralizar nodos logísticos críticos durante periodos de hasta tres semanas, afectando gravemente a la continuidad del negocio.



Impacto económico

IBM y el Ponemon Institute[6] estiman que el coste medio de una brecha de seguridad supera los **4 millones de dólares**, sin contar el impacto reputacional ni las sanciones regulatorias. Para una pyme, estos costes pueden resultar devastadores. Se revela que un incidente grave no solo afecta a la operativa física, sino que puede llegar a bloquear las comunicaciones con las entidades bancarias, paralizando los flujos financieros de la organización.



Impacto social

La disrupción de cadenas logísticas críticas, como las de alimentación, farmacéutica o energía, tiene consecuencias directas sobre la **población**. Los ataques a infraestructura crítica tienen el potencial de generar **crisis humanitarias** en contextos de escalada geopolítica.

La **ciberseguridad** todavía **no** ocupa el **lugar estratégico** que merece en la mayoría de las organizaciones logísticas. Se observa que el cambio de mentalidad real solo se produce tras sufrir un incidente grave, y que incluso entonces la atención decae con rapidez.

> *"Cuando el problema es de un tercero, el cliente final no distingue quién es el responsable; para él, el problema es tuyo."*
>
> **Director de Supply Chain y Sostenibilidad, multinacional alimentaria**

---

[6] IBM Cost of a Data Breach 2025: https://www.ibm.com/reports/data-breach

4.3. Ecosistema de proveedores y clientes

La **cadena de suministro** contemporánea es un **ecosistema hiperconectado** en el que la postura de seguridad de cada actor condiciona la del conjunto. La caída de un **único proveedor** tecnológico o logístico puede **propagarse de forma inmediata** a todo el ecosistema de organizaciones que dependen de él.

Esta interdependencia convierte la **gestión del riesgo de terceros** en uno de los grandes **retos operativos** de la actividad, especialmente en ecosistemas que superan el millar de proveedores, donde la auditoría contractual exhaustiva resulta inalcanzable.

Los mecanismos actuales muestran **limitaciones** evidentes: los cuestionarios de seguridad son con frecuencia tan superficiales que actúan más como descargo de responsabilidad legal que como mecanismo real de control, y para las micropymes y autónomos del transporte los requisitos formales son directamente impracticables, lo que lleva a sustituir la auditoría directa por herramientas de monitorización externa proactiva.

Frente a este escenario, algunos operadores han optado por endurecer significativamente sus propios procesos: un operador logístico internacional describió cómo el análisis de ciberseguridad ha pasado de representar el 20% al 80% del proceso de habilitación de nuevos proveedores, descartando directamente a aquellos sin capacidad suficiente.

La experiencia práctica revela además fallos estructurales que solo afloran cuando el incidente ya ha ocurrido, como las copias de seguridad almacenadas en el mismo servidor de producción, o la constatación de que la recuperación no depende únicamente de restaurar los sistemas propios, sino de sincronizarlos con los de los terceros que también sufrieron el impacto, lo que alarga significativamente los plazos reales frente a los teóricos. Y cuando el fallo es de un tercero, el mercado no distingue responsabilidades: el daño reputacional recae íntegramente sobre la marca que da la cara ante el cliente final.



Para visibilizar el impacto real, se presentan a continuación casos concretos que ilustran la propagación sistémica de los ataques:

Incidentes internacionales de alto impacto

Puerto de Seattle (agosto 2024)[7]

Ataque ransomware del grupo Rhysida. Afectó a ~90.000 personas y comprometió sistemas del aeropuerto SEA-TAC. La respuesta incluyó el aislamiento de sistemas críticos, la activación de protocolos de continuidad manual y la colaboración con agencias federales de ciberseguridad.

Marks & Spencer, Co-op, Harrods y Dior (abril-mayo 2025)[8]

La caída de plataformas centralizadas paralizó a cientos de pequeños distribuidores y proveedores dependientes digitalmente. La lección: La concentración de dependencias tecnológicas en pocos proveedores amplifica exponencialmente el impacto de un ataque.

Chain IQ Group (2025)[9]

Brecha que expuso datos de más de 130.000 empleados pertenecientes a múltiples pyme clientes.

Miljödata, Suecia (agosto 2025)[10]

El ataque al proveedor tecnológico colapsó sistemas usados por más del 80% de los municipios, dejando inoperativas a decenas de empresas subcontratadas.

Impacto en el contexto español

España (2025)[6]

605 incidentes significativos en el segundo semestre. La mayoría de incidentes que afectaron a pymes se originaron en vulnerabilidades de terceros con acceso a sus sistemas.

El Corte Inglés (marzo 2025)[11]

Brecha de seguridad originada en un proveedor externo que permitió el acceso no autorizado a datos personales de clientes. La información comprometida incluyó datos identificativos y de contacto, así como números de tarjetas válidos únicamente para compras en El Corte Inglés. No se vieron afectados los sistemas internos ni las tarjetas bancarias.

Mango (octubre 2025)[12]

Acceso no autorizado a datos personales de clientes a través de un servicio externo de marketing. Los atacantes obtuvieron información utilizada en campañas comerciales (nombre, país, código postal, teléfono y correo electrónico), sin impacto en la operativa de la compañía ni compromiso de datos bancarios o credenciales de acceso.

España registró un **crecimiento sostenido** de incidentes de **ciberseguridad** en **2025** (**+26%** en comparación con **2024**[13]), en un contexto europeo donde los ataques con origen en la cadena de suministro digital se **duplicaron** respecto a **2024**[14].

---

[7] Port of Seattle — "Port Cyberattack Archive" (comunicado oficial) https://www.portseattle.org/news/port-cyberattack-archive

[8] Computer Weekly — "Four arrested in M&S cyber attack investigation" https://www.computerweekly.com/news/366627353/Four-arrested-in-MS-cyber-attack-investigation

[9] Chain IQ — "Cyber-Attack Chain IQ Group AG" (comunicado oficial de la empresa) https://chainiq.com/news/cyber-attack-chain-iq-group-ag/

[10] The Record — "A suspected ransomware attack on Miljödata..." https://therecord.media/sweden-municipalities-ransomware-software

[11] https://www.channelpartner.es/seguridad/principales-ciberataques-en-espana-en-2025/

[12] The Record (Recorded Future News) — "Mango says some customer information exposed in cyber incident" https://therecord.media/mango-fashion-retaier-data-breach

[13] INCIBE. (2026). Balance de ciberseguridad 2025. https://www.incibe.es

[14] Cipher (2026). Ataques a la cadena de suministro: análisis 2025 y tendencias 2026. Grupo Prosegur. https://www.cipher.com/es_ES/recursos/ataque-cadena-suministro

4.4. Principales vulnerabilidades

4.4.1. Tipología de ataques

Los ataques contemporáneos se caracterizan por su capacidad para **causar daños progresivos**, su **rapidez de propagación** y la **dificultad para detectarlos**. Entre las amenazas más recurrentes en el entorno logístico figuran:



Phishing, Phishing-as-a-Service y spear phishing con IA

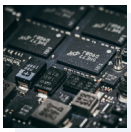
Campañas de ingeniería social de alta precisión, incluyendo técnicas avanzadas como ClickFix, que **suplantan identidades empresariales** y explotan errores humanos para obtener accesos iniciales. Los ciberdelincuentes utilizan **IA generativa** para crear campañas extremadamente difíciles de detectar. El phishing representa el **60%** de los accesos iniciales en organizaciones europeas[15].

Además, se observa la creciente proliferación de campañas de ingeniería social altamente sofisticadas basadas en **clonación de voz mediante IA** con tasas de éxito que pueden superar el 90% en ataques de suplantación de directivos orientados a fraude financiero.



Ataques DDoS (denegación distribuida de servicio)

Saturación de servidores o redes mediante tráfico masivo para interrumpir la disponibilidad de plataformas críticas. Los ataques dirigidos a infraestructura logística aumentaron un **61%** durante 2025, con una creciente sofisticación impulsada por automatización e IA generativa.



APTs, manipulación de componentes y ataques a la cadena de suministro

Operaciones persistentes que incluyen la **modificación de software, firmware o lógica de control** en Controladores Lógicos Programables (PLC) y otros activos OT, con potencial para generar daños físicos directos en líneas de producción o infraestructura crítica.



Compromiso de identidades, infostealers y privilegios administrativos

Robo de credenciales mediante malware especializado y su posterior uso para acceder lateralmente a sistemas a lo largo de toda la cadena logística. La ausencia de controles de acceso adecuados está detrás del **97%** de los incidentes relacionados con IA[7].



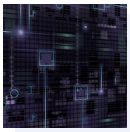
Explotación de vulnerabilidades en APIs y aplicaciones web

Los portales de proveedores, plataformas EDI y marketplaces B2B constituyen superficies de ataque críticas. APIs mal configuradas, inyecciones SQL y errores operativos facilitan **movimientos laterales** hacia sistemas internos sin activar mecanismos de alerta, favoreciendo brechas de datos a gran escala.



Ransomware y extorsión dirigidos a la producción

Cifrado de activos operativos y exfiltración previa de información sensible para maximizar el impacto económico y reputacional mediante doble extorsión. En entornos industriales OT, el tiempo medio de permanencia alcanzó los 42 días en 2025, y el sector manufacturero concentró más de dos tercios de las víctimas[4].



Fugas de datos y robo de propiedad intelectual

Extracción silenciosa y prolongada de información estratégica, como datos operativos, planos, fórmulas o contratos, a menudo sin provocar disrupciones visibles. En estos casos, el objetivo principal no es la paralización inmediata, sino la exfiltración discreta sin alertar a la organización.

---

[15] ENISA. (2025). Cybersecurity threat landscape 2025: Key takeaways for SMEs.

Por otro lado, surge un riesgo creciente derivado del **"Shadow IT"**, donde personal no técnico utiliza herramientas de IA generativa para desarrollar, por ejemplo, aplicaciones operativas que facilitan su labor, exponiendo involuntariamente datos sensibles de la compañía.

> *"La ciberseguridad, si le sumas la inteligencia artificial, ya es una ola muy salvaje que se nos viene encima y abre muchos frentes."*
>
> **Responsable de Seguridad de la Información, empresa logística**

4.4.2. El dato como activo crítico

En el entorno digital actual, el dato se ha convertido en el **activo más valioso** de la organización y, simultáneamente, en su **principal vector de ataque**. IBM y el Ponemon Institute[7] identifican la información personal identificable de clientes como el tipo de dato más frecuentemente comprometido, presente en el 53% de las brechas analizadas sobre 600 organizaciones en 17 sectores.

Las organizaciones que no controlan quién accede a qué datos, desde dónde y con qué propósito, no están gestionando un riesgo técnico: están dejando abierta la puerta principal de su cadena de suministro.

La **IA está presente en uno de cada seis ataques**, principalmente para **phishing** (37%) y suplantación mediante **deepfakes** (35%). Esta realidad obliga a replantear la gobernanza del dato no como un ejercicio de cumplimiento regulatorio sino como una decisión estratégica.



"La ciberseguridad es como el nivel de inglés: todo el mundo dice que lo tiene alto hasta que le toca hablar."

Cybersecurity, empresa tecnológica

4.4.3. El factor humano: el eslabón más vulnerable

El **componente humano** es el **eslabón más vulnerable** de la cadena de ciberseguridad. No obstante, cuando se le prepara de forma continua y se le dota de criterio para actuar, se convierte también en su **línea de defensa más difícil de neutralizar**.

El elemento humano estuvo presente en el 60% de las brechas analizadas, ya sea por error, manipulación o uso indebido de privilegios. Data Breach Investigations Report de Verizon Business (2025).

El sector enfrenta además una crisis silenciosa: El **déficit global de talento en ciberseguridad** se estima entre 2,8 y 4,8 millones de profesionales cualificados, y dos de cada tres organizaciones reportan carencias de habilidades de moderadas a críticas[16].

67%

de las organizaciones reportó escasez de profesionales de ciberseguridad en 2024[18]

58%

considera que la brecha de habilidades pone a su organización en riesgo significativo ante ataques sofisticados[7]

74%

de los profesionales del sector percibe el panorama de amenazas como el más desafiante de los últimos cinco años[7]

En la actividad logística el factor humano adquiere una dimensión adicional: una parte relevante de la plantilla -conductores, operarios de almacén, personal temporal y rotativo- no utiliza herramientas informáticas en su día a día, lo que hace ineficaces los programas de formación tradicionales basados en correo electrónico o vídeos. Empresas del sector han optado por integrar píldoras de ciberseguridad en el proceso de onboarding, implementar soluciones de gestión de dispositivos móviles (MDM) en dispositivos móviles de conductores, y sustituir los clásicos envíos de phishing simulado por llamadas de voz generadas con IA, donde el índice de caída supera el 90%. El personal temporal y rotativo es señalado por el sector como uno de los vectores de entrada más vulnerables, por recibir menos formación y tener acceso transitorio a sistemas críticos.

Por otro lado, se confirma una tendencia a la relajación de la alerta una vez superado un incidente grave, lo que evidencia que la cultura de seguridad es a menudo reactiva y efímera si no se gestiona de forma permanente.

"La concienciación no es solo del comité de dirección, sino de todas las áreas de negocio. El conocimiento tiene que permear a todos."

Director de Sistemas de Información, empresa de transporte refrigerado.

[16] ISC2 Cybersecurity Workforce Study 2024: https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study

4.5. Prevención, monitorización y planes de contingencia para cadenas de suministro resilientes

La **ciberresiliencia** se perfila como la **pieza clave del nuevo enfoque de seguridad**. Prevenir ataques sigue siendo necesario, pero resulta insuficiente. Las organizaciones deben ser capaces de **absorber impactos, adaptarse con rapidez a situaciones adversas y restaurar sus funciones críticas** para garantizar la continuidad del servicio.

Los estudios más recientes demuestran que esta resiliencia es una capacidad dinámica que puede construirse mediante procesos organizativos deliberados, no únicamente mediante inversiones tecnológicas, y que las cadenas que invierten en capacidades de detección y respuesta obtienen tiempos de recuperación significativamente inferiores.

Un plan de contingencia efectivo en el contexto de la cadena de suministro debe contemplar: La identificación previa de los procesos y dependencias críticas (BIA), el establecimiento de protocolos de comunicación internos y externos, la definición de roles y responsabilidades en el momento del incidente, y la práctica periódica mediante ciberejercicios y simulaciones.

Sin embargo, la experiencia práctica revela que estos planes suelen ser puramente teóricos y presentan **fallos de diseño graves** -como el almacenamiento de copias de seguridad en los mismos entornos de producción que pretenden proteger- que solo afloran cuando el incidente ya ha ocurrido. La recomendación es clara: los planes de continuidad deben ir más allá del plano de IT, incluir alternativas operativas concretas y ser probados con regularidad. Una medida destacada por operadores del sector es la implantación de equipos de contingencia aislados en almacenes que permitan garantizar una operativa mínima -acceso a navegadores y bases de datos secundarias- ante un compromiso total de la red por ransomware. La comunicación es igualmente crítica; un retraso superior a una hora en informar a clientes y socios multiplica exponencialmente el daño reputacional.



Todo ello exige una figura de liderazgo a la altura del reto. El CISO no puede seguir siendo un técnico aislado en su departamento, sino que debe actuar como un aliado estratégico de la dirección, capaz de traducir los riesgos tecnológicos al lenguaje del negocio, construir alianzas en todos los niveles de la organización y mantener la tensión cultural entre incidentes. La formación continua, segmentada por perfil y apoyada en ejercicios reales -incluyendo simulaciones de phishing por voz con IA- se revela como la única vía sostenible para mantener el nivel de alerta.

Hay que focalizar el esfuerzo en la resiliencia y la recuperación, más que en la prevención.

> *"El CISO tiene que ir a los despachos como alguien que aporta valor, no como un técnico encerrado en su cuarto."*
>
> **Responsable de Seguridad de la Información, empresa logística.**

4.6. Tecnologías que habilitan la resiliencia

La incorporación de nuevas arquitecturas tecnológicas está transformando de forma profunda la manera en que las cadenas de suministro se protegen frente a ciberataques. En el contexto logístico, destacan las siguientes tecnologías:

- **Zero Trust Architecture (ZTA):** Elimina la confianza implícita y exige verificación continua de usuarios, dispositivos y proveedores bajo el principio «nunca confíes, siempre verifica». Resulta especialmente adecuada en cadenas con múltiples actores externos. Se apoya en mecanismos como autenticación multifactor, control de accesos, segmentación, sistemas IDS/IPS y protección perimetral, y se alinea con marcos como ISO 27001 o el ENS.

- **Automatización de la gestión de vulnerabilidades y revisión de software:** Herramientas que analizan de forma continua equipos, redes, aplicaciones y componentes de terceros para detectar debilidades antes de su explotación. En 2024, el 23,6 % de las vulnerabilidades conocidas explotadas lo fueron el mismo día o antes de su divulgación pública .

- **Detección y monitorización continuas (SOC/MDR):** Supervisión continua mediante SOC gestionados, SIEM (Security Information and Event Management, en español Gestión de Información y Eventos de Seguridad) y análisis de registros, que permite detectar anomalías y responder con rapidez. Estos servicios incorporan cada vez más técnicas de inteligencia artificial y machine learning, facilitando su adopción incluso en organizaciones con recursos limitados.

- **Plataformas de inteligencia sobre amenazas (CTI):** Sistemas que agregan y correlacionan indicadores de compromiso, campañas activas y vulnerabilidades emergentes, ofreciendo una visión continua del riesgo. Arisian et al. muestran que el intercambio de inteligencia dentro de un mismo sector genera un valor defensivo superior al esfuerzo individual.

- **Tecnologías de trazabilidad, integridad y seguridad de la información:** Soluciones basadas en firmas digitales y mecanismos de integridad que garantizan la autenticidad, el no repudio y la protección de la información intercambiada a lo largo de la cadena logística.

- **Gemelos digitales de seguridad:** Réplicas virtuales de la infraestructura logística que permiten simular ataques, evaluar impactos y probar contramedidas sin afectar a los sistemas productivos.

- **Ciberejercicios y simulaciones de incidentes:** Escenarios controlados que evalúan la capacidad real de detección, respuesta y coordinación ante incidentes, fortaleciendo la preparación organizativa. Kävrestad et al evidencian mejoras significativas en la conciencia situacional y la toma de decisiones.

- **Análisis de Impacto de Negocio (BIA) y continuidad operativa:** Metodologías que identifican procesos críticos, dependencias y tolerancia a la interrupción, permitiendo anticipar efectos en cascada y definir planes de continuidad y recuperación.

Estas tecnologías no actúan de forma aislada, sino que se integran de manera transversal para cubrir prevención, detección y respuesta. En conjunto, permiten abordar la ciberresiliencia de forma integrada, teniendo en cuenta la complejidad y las múltiples dependencias propias de las cadenas de suministro logísticas.

En este ecosistema tecnológico, la IA ocupa un lugar dual: al mismo tiempo que democratiza el desarrollo de amenazas sofisticadas y amplía la superficie de ataque, se revela como una herramienta esencial para automatizar la vigilancia, mejorar la detección de anomalías y escalar la revisión de proveedores sin necesidad de aumentar los equipos.

---

[17] Black Kite 2025 Supply Chain Vulnerability Report: https://content.blackkite.com/ebook/2025-supply-chain-vulnerability-report.

[18] Arisian, S., Halat, K., Hafezalkotob, A., & Maskey, R. (2025). Coopetitive resilience: Integrating cyber threat intelligence platforms in critical supply chains. Transportation Research Part E, 197, 103985.

[19] Kävrestad, J., Johansson, S., & Bergström, E. (2025). Using tabletop exercises to raise cybersecurity awareness of decision-makers. En Critical Information Infrastructures Security: CRITIS 2024 (pp. 191–203). Springer.

En el extremo opuesto de la sofisticación, las soluciones MDM permiten llevar la concienciación y los protocolos de seguridad directamente al personal deslocalizado -conductores, operarios de almacén, personal temporal- a través de formatos digitales breves y adaptados, cerrando así una de las brechas más persistentes de la actividad logística.

> *"Da igual lo que inviertas, lo que va a pasar va a pasar."*
>
> **Head de Ciberseguridad, empresa retail**



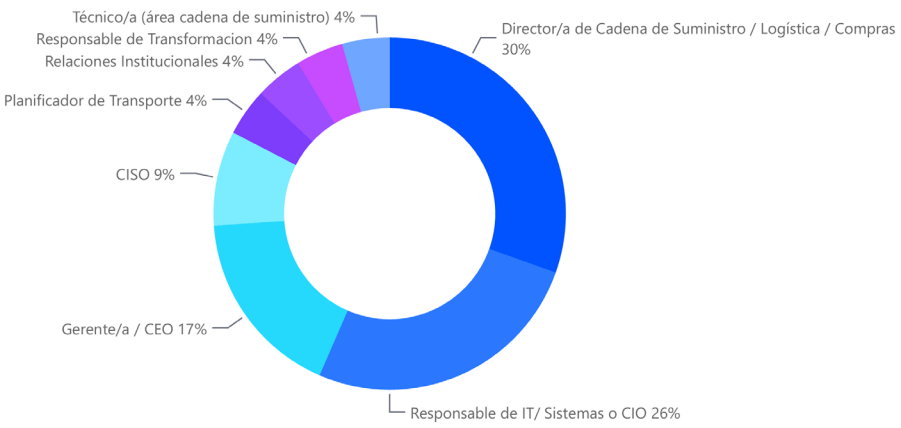
5. ANÁLISIS DE LA ENCUESTA DE CIBERSEGURIDAD EN LAS CADENAS DE SUMINISTRO

5.1. Perfil de la muestra

35%	35%	17%	4%	4%	4%
Fabricación / Producción	Transporte / Logística	Retail	Consultoría	Investigación	Tecnología / Software

Distribución por función

El perfil de los respondientes se concentra en posiciones con responsabilidad directa sobre la cadena de suministro y los sistemas de información, lo que aporta validez a las respuestas relativas a madurez tecnológica y gestión de proveedores.



El **52%** pertenece a organizaciones de **más de 250 empleados**, lo que implica que probablemente los resultados sobreestiman la madurez media real del sector, mayoritariamente compuesto por pymes. El tamaño de la muestra es en sí mismo un diagnóstico; una de las principales conclusiones es que la ciberseguridad sigue siendo en 2026 un tema periférico en la agenda logística.

La ciberseguridad sigue siendo en 2026 un tema periférico en la agenda logística, solo el 43% de las organizaciones dispone de una estrategia formal de ciberseguridad para su cadena de suministro.

5.2. Estrategia y percepción del riesgo

Solo el **43% de los encuestados dispone de una estrategia formal de ciberseguridad** para su cadena de suministro, frente a un 43% que no la tiene y un 13% en desarrollo. Si organizaciones de mayor tamaño y capacidad de inversión solo alcanzan esta cifra, cabe presumir un porcentaje considerablemente menor en el conjunto de la actividad.

Realizando el análisis por sector, Fabricación y Producción presenta los niveles más bajos de respuesta institucional ante el riesgo de ciberataque. Por su parte, **Retail junto a Transporte y Logística** son los sectores que se encuentran **más concienciados** ante el riesgo de amenaza de ciberseguridad.

El análisis por perfil no muestra diferencias significativas en la percepción del riesgo entre los distintos perfiles profesionales. Sin embargo, sí se observan diferencias relevantes según el tamaño de la empresa. En particular, el **67% de las grandes empresas** afirma contar con una **estrategia formal de ciberseguridad** para la cadena de suministro, frente al **0%** de las empresas **medianas**.

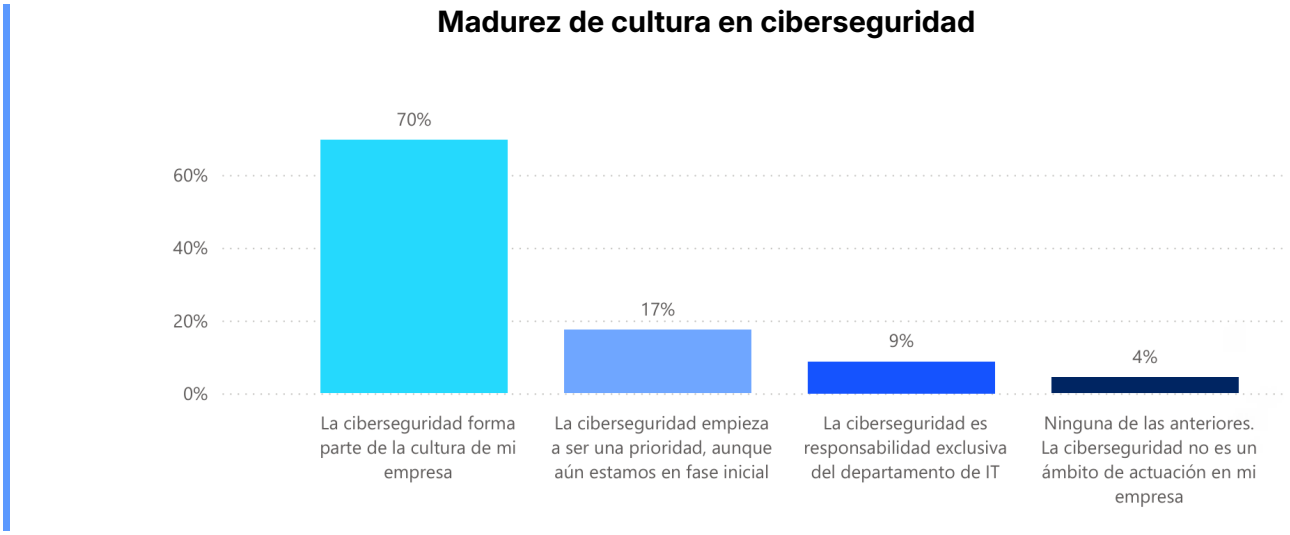
La percepción de **exposición geopolítica** es llamativamente contenida: solo el **9%** reconoce una exposición significativa, frente al 97% de nivel de amenaza global señalado por Everstream Analytics (2026)[2], lo que apunta a un déficit de visibilidad sobre las dependencias de la propia cadena más que a una exposición real reducida. El **26%** declara haber sufrido **al menos un incidente en los últimos 24 meses**, cifra consistente con el incremento del 61% en ciberataques a transportistas durante 2025.



5.3. Cultura organizativa y factor humano

El **70% percibe que la ciberseguridad forma parte de la cultura de su empresa**. Los indicadores operativos matizan este optimismo: solo el **48%** considera que su **personal sabría actuar** ante un incidente, un **22%** no ha **impartido ninguna formación en el último año**, y apenas el **52%** ha realizado **simulacros de ciberataque**. En el lado positivo, el **78% incentiva activamente el reporte de incidentes**, y el **44% forma regularmente al personal involucrado en gestión de proveedores**. La cultura percibida va claramente por delante de la capacidad de respuesta entrenada.







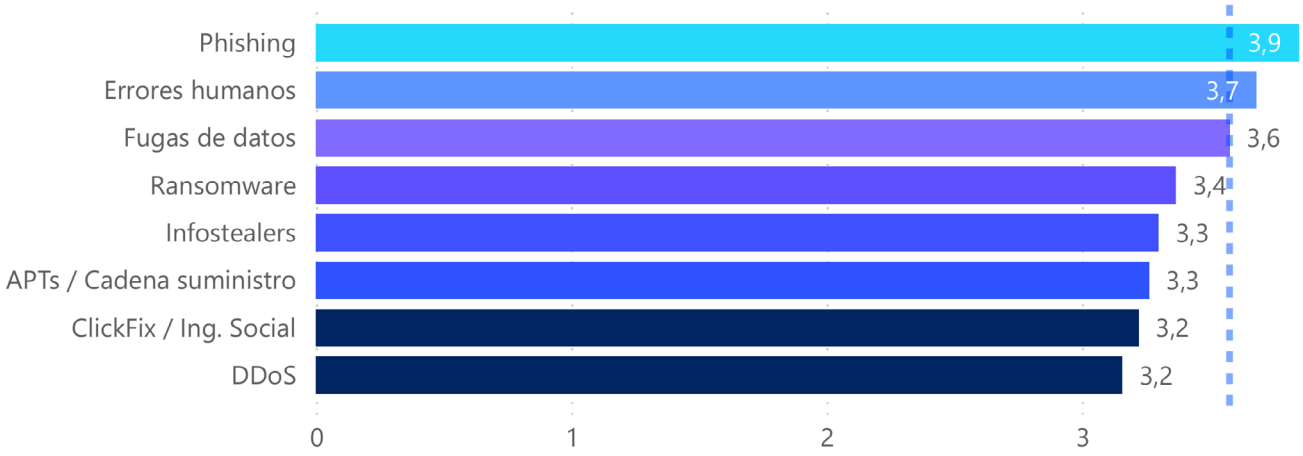
La cultura percibida va claramente por delante de la capacidad de respuesta entrenada. El 70% considera que la ciberseguridad forma parte de la cultura corporativa, pero únicamente el 48% cree que el personal sabría actuar correctamente ante un incidente.

5.4. Amenazas e inteligencia artificial

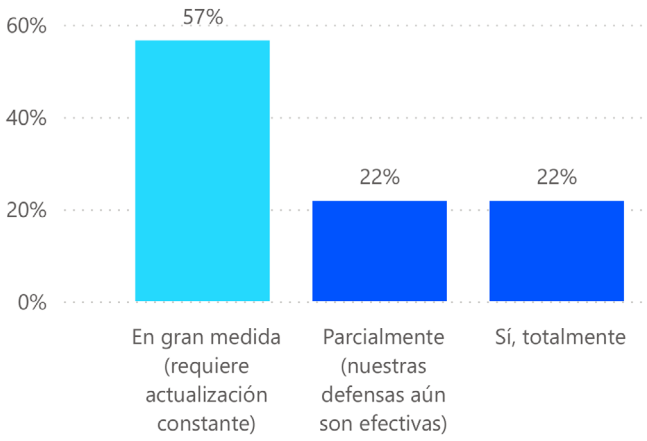
El **phishing** encabeza la jerarquía de preocupación (3,9 sobre 5), seguido de los **errores humanos** (3,7) y las **fugas de datos** (3,6), en plena coherencia con el marco teórico del estudio. Las amenazas más avanzadas -ClickFix, APTs, DDoS- concentran los mayores porcentajes de encuestados que declaran no saber valorarlas, lo que revela una brecha de comprensión sobre el frente de amenazas más sofisticado. Respecto a la **IA, el 78% la percibe como amenaza** y el 57% considera que sus **defensas requieren actualización constante**, pero la protección basada en IA/ML resulta ser la medida peor valorada de todo el cuestionario (2,7 sobre 5): la brecha entre amenaza reconocida y capacidad defensiva desplegada es la más urgente de cerrar.

Nivel de preocupación por tipo de amenaza

***1:** muy poco preocupante; **5:** muy preocupante*



Impacto de la IA en ciberdelincuencia sobre las defensas actuales



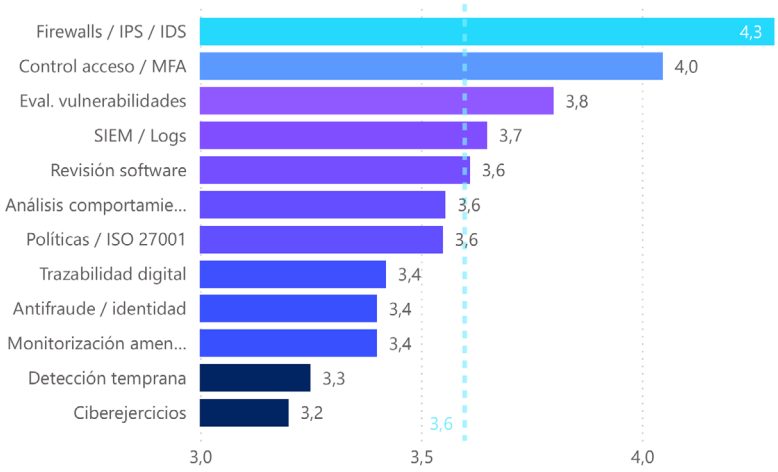
La brecha entre amenaza reconocida y capacidad defensiva desplegada es la más urgente de cerrar.

5.5. Madurez en la implementación de medidas

Las **medidas más tradicionales -firewalls/IPS/IDS** (4,3/5) y **control de acceso/MFA** (4,0/5)- son las mejor implantadas, mientras que la detección temprana (3,2/5) y los ciberejercicios (3,3/5) se encuentran a la cola. En el bloque de **medidas colaborativas y de gobernanza**, la continuidad de negocio (3,1/5) es la segunda peor valorada del conjunto, y la protección basada en IA/ML (2,7/5) la última de todas. Por su parte, las mejores valoradas son la **interacción con socios** (3,4/5) y el **intercambio de información** (3,4/5). El patrón es consistente: las organizaciones están mejor protegidas frente a amenazas conocidas que preparadas para detectar, responder y recuperarse ante incidentes reales.

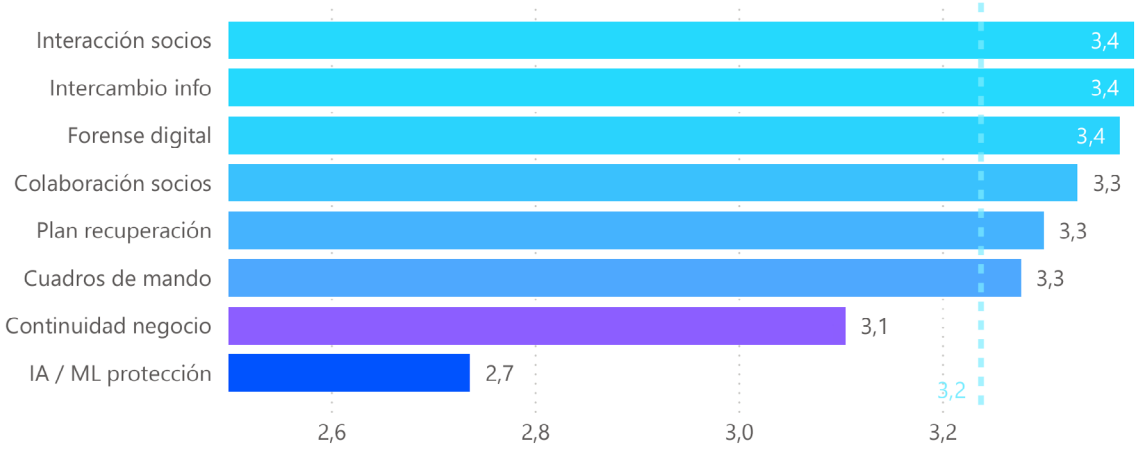
Medidas Técnicas - Implantación media

1: *muy poco implantado;* ***5:*** *muy implantado*



Medidas Colaborativas y de Gobernanza - Implantación Media

1: *muy poco implantado;* ***5:*** *muy implantado*

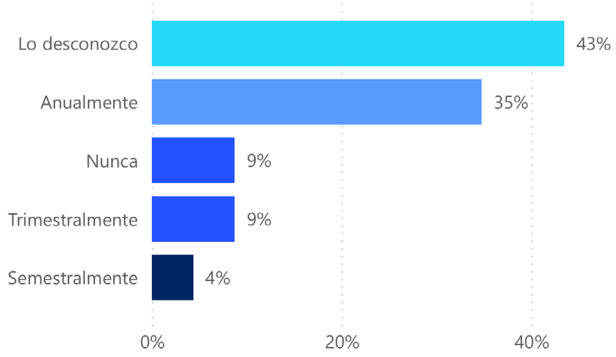


5.6. Gestión del riesgo de proveedores

El **48% no realiza auditorías periódicas de ciberseguridad a sus proveedores estratégicos**, y solo el **39% exige requisitos mínimos de ciberseguridad en los procesos de aprovisionamiento**. El dato más revelador: el 44% desconoce con qué frecuencia se revisan los riesgos de proveedores en su propia organización, un porcentaje que supera al de quienes afirman hacerlo anualmente (35%). La ausencia de visibilidad interna sobre los propios procesos de control es tan problemática como la ausencia del control mismo. El **57% de las empresas encuestadas verifica transacciones críticas con proveedores**, aunque casi un tercio desconoce si dicha verificación se realiza.

El 57% de las empresas encuestadas verifica transacciones críticas con proveedores, aunque casi un tercio desconoce si dicha verificación se realiza.

Frecuencia de revisión de riesgos de proveedores y terceros

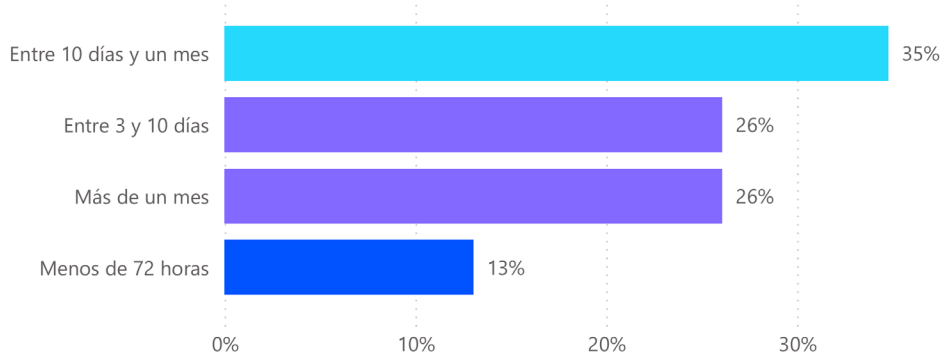




5.7. Impacto potencial: continuidad y resiliencia financiera

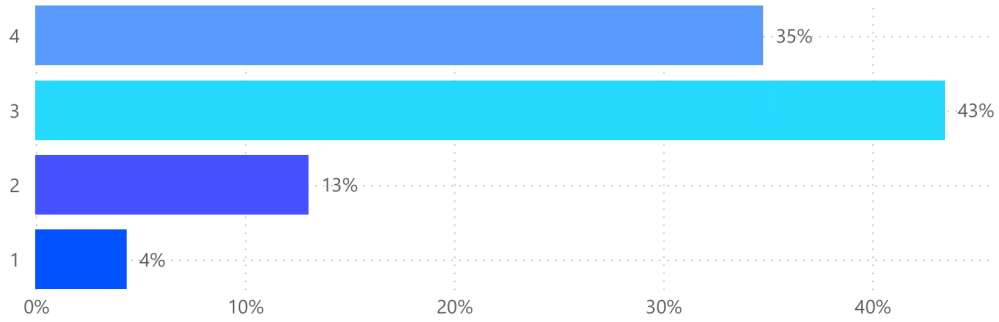
El **78% reconoce que al menos una parte relevante de su operativa se detendría ante un ataque a un proveedor logístico crítico**, confirmando desde la propia experiencia declarada la propagación sistémica descrita en el estudio. La fragilidad financiera es igualmente significativa: el **39% dispondría de menos de 10 días de margen** de tesorería ante una parada total, resultado obtenido sobre una muestra sesgada hacia empresas grandes, lo que sugiere una situación aún más crítica en el conjunto del sector. El **impacto** estimado sobre la confianza de socios y clientes se sitúa en una media de **3,14 sobre 5**, con la mayoría de encuestados situándolo entre niveles moderado y alto.

¿Cuánto aguanta la tesorería ante una parada total?

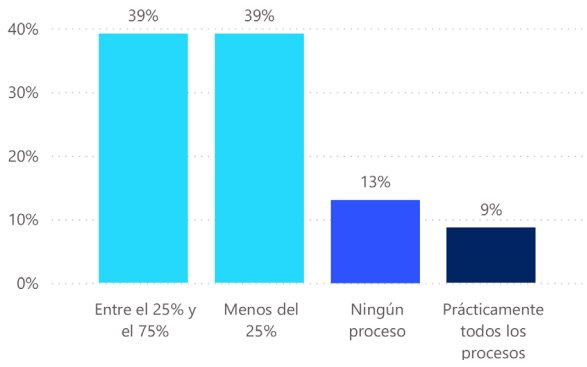


Impacto estimado de una brecha de confianza de socios

***1:** muy bajo impacto; **5:** muy alto impacto*



% de parada en la empresa ante un ataque a un proveedor logístico crítico



La resiliencia financiera es limitada: el 39% de las empresas no podría sostener una interrupción total durante más de 10 días.

"En la cadena de suministro la clave es la colaboración. No hay que avergonzarse de pedir ayuda cuando te ocurre algo; si lo compartimos, el golpe es más llevadero para todos."

Head de Ciberseguridad, empresa retail

La actividad logística confirma lo recogido en este estudio. El cambio de mentalidad real, según los profesionales consultados, solo se produce tras sufrir un incidente grave, y la atención decae con rapidez una vez superada la crisis. El **CISO emerge como figura clave** no como guardián técnico, sino como un traductor entre el mundo tecnológico y el negocio: alguien que habla el lenguaje de la dirección, construye alianzas internas y mantiene la tensión organizativa entre incidentes.

La ciberseguridad deja de ser un coste para convertirse en una ventaja competitiva y en una condición de acceso a mercados y colaboraciones con grandes operadores que exigen cada vez más a sus socios de cadena. Las organizaciones que comprendan esto antes que sus competidores no solo estarán mejor protegidas; estarán mejor posicionadas.



"Hay que vigilar, avisar y cooperar. Tenemos un déficit cultural que arrastramos desde los años 2000 y que aún no hemos superado."

Cybersecurity, empresa tecnológica



6. DESAFÍOS Y OPORTUNIDADES DE FUTURO

RETOS

A pesar de los avances regulatorios y tecnológicos, persisten retos significativos cuya resolución determinará el grado de ciberresiliencia alcanzable por el ecosistema logístico en el horizonte 2026-2030:

01 La **limitada visibilidad sobre proveedores de proveedores a partir del segundo nivel** sigue siendo el principal obstáculo operativo para una gestión eficaz del riesgo cibernético en la cadena.

02 La **tensión entre la necesaria transparencia sobre vulnerabilidades y la protección de secretos comerciale**s dificulta la colaboración entre competidores del mismo sector para afrontar amenazas comunes.

03 La necesidad de adaptar las soluciones técnicas y los marcos regulatorios a las **capacidades operativas y financieras reales de las pymes**.

04 La **cuantificación de la resiliencia** continúa siendo un dominio metodológicamente inmaduro, lo que dificulta la justificación de inversiones ante la dirección.

05 El **déficit de talento especializado**, cuya brecha se amplía a mayor velocidad de la que el sistema formativo puede cerrar.

OPORTUNIDADES E INNOVACIÓN

En este contexto, las siguientes líneas de innovación se configuran como vías estratégicas para reducir la brecha de ciberresiliencia:

01 **Desarrollo de modelos predictivos basados en IA** para la identificación anticipada de vulnerabilidades y la simulación de impactos en cascada a lo largo de la cadena.

02 **Tecnologías de colaboración segura** que permiten compartir inteligencia sobre amenazas con socios y competidores sin exponer información estratégica propia.

03 **Automatización inteligente de procesos de auditoría a proveedores**, reduciendo el coste y tiempo de cumplimiento con estándares como ISO 27036 o los requisitos de NIS2.

04 **Provisión de servicios de ciberseguridad gestionada** (MSSP/MDR) específicamente diseñados para pymes con modelos de precios accesibles y escalables.

05 **Integración de señales de riesgo cibernético en tiempo real** dentro de los sistemas de planificación de la cadena de suministro (S&OP, control towers).

Con todo, el sector es claro:

la **ciberseguridad** debe integrarse como un **indicador clave de negocio** en los comités de dirección, al mismo nivel que los indicadores operativos o financieros, dejando de ser percibida como un asunto exclusivo de los equipos técnicos.

Más allá de la madurez interna de cada organización, emerge con fuerza la idea de que la **resiliencia es, por naturaleza, colectiva**. Los ataques sufridos por competidores directos deben interpretarse como amenazas propias, y el intercambio de inteligencia sobre amenazas entre empresas del mismo ecosistema -incluso entre competidores- debe pasar de ser una práctica excepcional a convertirse en la norma. **Un ataque a cualquier actor de la cadena es una amenaza potencial para todos los que dependen de ella.**



7. CONCLUSIONES FINALES

El análisis desarrollado a lo largo de este trabajo permite extraer una serie de conclusiones que reflejan tanto los avances como las carencias que definen hoy la madurez en ciberseguridad de la actividad logística.

1. La ciberseguridad ha pasado de ser una función técnica a un elemento estratégico, pero la adopción formal sigue sin ser mayoritaria.

El 78% de las organizaciones reconoce que un ciberataque a un proveedor crítico afectaría directamente a su propia operativa, sin embargo, solo el 43% dispone de una estrategia formal de ciberseguridad para su cadena de suministro, otro 43% no la tiene y un 13% la tiene en desarrollo. Esta brecha entre percepción de riesgo y respuesta estratégica evidencia que la ciberseguridad debe consolidarse como prioridad de negocio, y no únicamente tecnológica.

---

2. La cultura declarada de seguridad es superior a la capacidad real de respuesta.

El 70% considera que la ciberseguridad forma parte de la cultura corporativa, pero únicamente el 48% cree que el personal sabría actuar correctamente ante un incidente. Existe, por tanto, una brecha relevante entre percepción cultural y preparación operativa.

---

3. El factor humano y el phishing son las principales amenazas percibidas por las organizaciones.

Los errores humanos obtienen una valoración de riesgo de 3,7 sobre 5, coherente con la evidencia externa de que el 60% de las brechas de seguridad incluye un componente humano. El phishing, con 3,9 sobre 5, es la amenaza mejor reconocida, consolidándose como la principal preocupación inmediata de las organizaciones logísticas.

---

4. Las empresas protegen mejor el acceso que la detección temprana y la respuesta ante incidentes.

Las medidas mejor implantadas son los firewalls y sistemas IDS/IPS (4,3/5) y el control de accesos con MFA (4,0/5), frente a niveles de madurez notablemente inferiores en detección temprana (3,2/5), continuidad de negocio (3,1/5) y protección basada en IA (2,7/5). Esto confirma una postura defensiva más preventiva que reactiva, y evidencia que alcanzar una verdadera ciberresiliencia exige avanzar simultáneamente en capacidades tecnológicas, mecanismos de gobernanza y desarrollo del talento.



5. La gestión del riesgo de proveedores es uno de los principales puntos críticos de la cadena.

El 48% no realiza auditorías periódicas de ciberseguridad a sus proveedores estratégicos y solo el 39% exige requisitos mínimos de ciberseguridad en los procesos de aprovisionamiento. La falta de controles y de visibilidad sobre terceros se traduce en una elevada vulnerabilidad operativa y financiera para toda la cadena.

---

6. La exposición geopolítica está claramente infravalorada por las empresas.

Solo el 9% de las organizaciones reconoce una exposición significativa a riesgos geopolíticos, mientras que la fragmentación geopolítica alcanza un 97% de nivel de amenaza para las cadenas de suministro globales según Everstream Analytics. La percepción empresarial se sitúa muy por debajo del riesgo identificado por los expertos internacionales.

---

7. La ciberresiliencia ya no depende únicamente de cada empresa, sino de la capacidad de colaboración de todo el ecosistema.

El 78% reconoce que un ciberataque a un proveedor logístico crítico afectaría directamente a su propia operativa, y el 57% verifica transacciones críticas con proveedores, aunque la interacción y el intercambio de información entre socios apenas alcanzan 3,4 sobre 5. Los riesgos ya no pueden gestionarse dentro de los límites de una sola organización: exigen una visión sistémica de la cadena (incluyendo entornos IT y OT y todos los niveles de proveedor), mecanismos de gobernanza con responsabilidades compartidas, y una cultura de seguridad transversal a toda la cadena de valor.

---

8. La madurez de la ciberseguridad en la actividad logística en 2026 sigue siendo limitada y desigual, lo que la convierte en una condición imprescindible para la continuidad del negocio.

A pesar de una percepción cultural relativamente positiva, persisten carencias importantes en formación, preparación operativa, detección temprana y capacidad de respuesta ante incidentes, especialmente en el uso de inteligencia artificial. Esta combinación de baja madurez y alta interdependencia implica que un solo incidente puede tener efectos sistémicos sobre la continuidad del negocio y la confianza de clientes y socios: la ciberseguridad ya no es una opción, sino una condición imprescindible para la supervivencia de la actividad logística.



8. DECÁLOGO

Buenas prácticas en ciberseguridad para la cadena de suministro



1. Mapear la superficie de exposición real

Identificar todos los actores con acceso a los sistemas propios (proveedores, subcontratistas, plataformas SaaS...) y evaluar el nivel de riesgo que cada uno introduce. Este análisis debe extenderse más allá del proveedor de primer nivel, incluyendo dependencias tecnológicas que habitualmente quedan fuera del radar de auditoría. No es posible gestionar lo que no se conoce, y la mayoría de los ataques entran por eslabones que la organización no había identificado como críticos.

2. Integrar el riesgo cibernético en la selección y gestión de proveedores

La ciberseguridad debe ser un criterio explícito en los procesos de aprovisionamiento, junto al coste, la calidad y el plazo. La incorporación de cuestionarios de madurez digital, cláusulas contractuales de seguridad y auditorías periódicas a proveedores críticos es una práctica imprescindible en cadenas maduras.

3. Adoptar una arquitectura de confianza cero (Zero Trust)

La arquitectura de confianza cero elimina la confianza implícita en usuarios, dispositivos y sistemas, independientemente de si operan dentro o fuera de la red corporativa. Su principio rector es claro: Nunca confiar, siempre verificar. Su implantación debe planificarse de forma escalonada, priorizando los accesos más críticos.

4. Priorizar la detección y la respuesta frente a la prevención exclusiva

Prevenir ataques es necesario pero insuficiente. La inversión en capacidades de detección temprana permite identificar amenazas antes de que se materialicen en crisis. El tiempo medio de permanencia de un atacante en entornos industriales supera los 40 días: Cada día sin detección es un día de exposición activa.

8. DECÁLOGO

Buenas prácticas en ciberseguridad para la cadena de suministro



5. Desarrollar y entrenar el plan de respuesta ante incidentes

Disponer de un plan de continuidad no es suficiente si no se practica. Los ciberejercicios y simulaciones permiten identificar brechas en los protocolos y construir memoria organizativa colectiva antes de que el incidente real ocurra. El Análisis de Impacto de Negocio (BIA) debe identificar previamente qué procesos y dependencias de terceros son críticos para la continuidad operativa.

6. Proteger el dato como activo estratégico

La información comprometida aparece en más de la mitad de las brechas de seguridad. La implantación de políticas de acceso con mínimo privilegio, cifrado en tránsito y en reposo, y auditoría continua sobre quién accede a qué datos constituye la base de una gobernanza del dato eficaz. Las copias de seguridad aisladas y probadas periódicamente son la medida más eficaz para evitar el pago de rescates.

7. Convertir el factor humano en la primera línea de defensa

El elemento humano está presente en el 60% de las brechas. La formación continua y los canales de denuncia no punitivos transforman la vulnerabilidad potencial en capacidad defensiva. La ciberseguridad es una responsabilidad que atraviesa todos los niveles de la organización, no únicamente los departamentos técnicos. Además, los proveedores de soluciones deben entender los procesos y restricciones reales del negocio logístico para proponer herramientas técnicas. Por otro lado, los socios tecnológicos deben actuar como “traductores” entre los departamentos de IT y los de Operaciones, facilitando el entendimiento mutuo para evitar brechas.

8. Cumplir la regulación como punto de partida, no como destino

NIS2, CRA, DORA y el ENS establecen el suelo normativo mínimo, no el techo de madurez. Las organizaciones que gestionan la regulación como un ejercicio de cumplimiento formal pierden la oportunidad de convertirla en una palanca de mejora real.

8. DECÁLOGO

Buenas prácticas en ciberseguridad para la cadena de suministro



9. Colaborar con el ecosistema: La resiliencia es colectiva

Ninguna organización puede ser resiliente en solitario si sus proveedores y socios no lo son. Compartir inteligencia sobre amenazas con actores del mismo sector y exigir a los proveedores críticos niveles mínimos de madurez en ciberseguridad son prácticas que fortalecen la cadena en su conjunto.

10. Integrar la ciberseguridad en la estrategia de negocio

La ciberseguridad deja de ser un coste cuando se gestiona como una capacidad estratégica. Las organizaciones que integran el riesgo cibernético en sus decisiones de planificación y diseño de cadena no solo están mejor protegidas: están mejor posicionadas para crecer y generar confianza con grandes operadores. La pregunta ya no es si invertir en ciberseguridad, sino cuánto cuesta no hacerlo.

9. BIBLIOGRAFÍA

Publicaciones académicas

Alguirat, I., Lehyani, F., & Zouari, A. (2025). Digital twins in supply chain management: A review of their role in boosting operational efficiency. Business Process Management Journal, 1–28.

Arisian, S., Halat, K., Hafezalkotob, A., & Maskey, R. (2025). Coopetitive resilience: Integrating cyber threat intelligence platforms in critical supply chains. Transportation Research Part E, 197, 103985.

Bode, C., & Wagner, S. M. (2015). Structural drivers of upstream supply chain complexity and the frequency of supply chain disruptions. Journal of Operations Management, 36, 215–228.

Ghadge, A., Weiss, M., Caldwell, N., & Wilding, R. (2020). Managing cyber risk in supply chains: A review and research agenda. Supply Chain Management: An International Journal, 25(2), 223–240.

Herburger, M., Wieland, A., & Hochstrasser, C. (2024). Building supply chain resilience to cyber risks: A dynamic capabilities perspective. Supply Chain Management: An International Journal, 29(7), 28–50.

Ivanov, D., & Dolgui, A. (2021). A digital supply chain twin for managing the disruption risks and resilience in the era of Industry 4.0. Production Planning & Control, 32(9), 775–788.

Kaur, H., Gupta, M., & Singh, S. P. (2024). Integrated model to optimize supplier selection and investments for cyber resilience in digital supply chains. International Journal of Production Economics, 275, 109362.

Kävrestad, J., Johansson, S., & Bergström, E. (2025). Using tabletop exercises to raise cybersecurity awareness of decision-makers. En Critical Information Infrastructures Security: CRITIS 2024 (pp. 191–203). Springer.

Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: An interdisciplinary review and framework proposal. International Journal of Information Security, 24, 119.

Melnyk, S. A., et al. (2022). New challenges in supply chain management: Cybersecurity across the supply chain. International Journal of Production Research, 60(1), 162–183.

Nygård, A., & Katsikas, S. (2022). SoK: Combating threats in the digital supply chain. ACM International Conference Proceeding Series.

Pickren, R., Shekari, T., Zonouz, S., & Beyah, R. (2024). Compromising industrial processes using web-based programmable logic controller malware. NDSS 2024.

Queiroz, M. M., et al. (2022). Impacts of epidemic outbreaks on supply chains. Annals of Operations Research, 319(1), 1159–1196.

Schmitt, M., & Flechais, I. (2024). Digital deception: Generative artificial intelligence in social engineering and phishing. Artificial Intelligence Review, 57, 324.

Simon, J., & Omar, A. (2020). Cybersecurity investments in the supply chain: Coordination and a strategic attacker. European Journal of Operational Research, 282(1), 161–171.

Wallis, T., Johnson, C., & Khamis, M. (2021). Interorganizational cooperation in supply chain cybersecurity. Information Security Journal: A Global Perspective, 30(4), 195–211.

Windelberg, M. (2016). Objectives for managing cyber supply chain risk. International Journal of Critical Infrastructure Protection, 12, 4–11.

Informes institucionales y organismos de referencia

Black Kite. (2025). 2025 supply chain vulnerability report.

Dragos. (2026). 2026 OT/ICS cybersecurity year in review.

ENISA. (2025). Cybersecurity threat landscape 2025: Key takeaways for SMEs.

Everstream Analytics. (2026). Supply chain risk report 2026.

IBM & Ponemon Institute. (2025). Cost of a data breach report 2025.

ISC2. (2024). 2024 Cybersecurity workforce study.

NIST. (2020). Special publication 800-207: Zero trust architecture.

NIST. (2022). Special publication 800-161r1: Cybersecurity supply chain risk management practices.

NIST. (2025). Using business impact analysis to inform risk prioritization and response (NIST IR 8286D).

NTT DATA. (2026). España sufre tres ciberataques graves al día, con la industria en el punto de mira.

Port of Seattle. (2025). Port of Seattle providing notice to individuals affected by fall 2024 cyberattack.

SOCRadar. (2026). Top 10 supply chain attacks of 2025.

Verizon Business. (2025). 2025 Data Breach Investigations Report (DBIR).

World Economic Forum. (2024). The global risks report 2024.

Marcos normativos y regulatorios

ISA/IEC. (2018). ISA/IEC 62443 – Security for industrial automation and control systems.

ISO. (2021). ISO/IEC 27036-1:2021 – Cybersecurity: Supplier relationships.

ISO. (2022). ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection.

Ministerio de la Presidencia. (2022). Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Parlamento Europeo y del Consejo de la UE. (2022a). Directiva (UE) 2022/2555 (NIS2).

Parlamento Europeo y del Consejo de la UE. (2022b). Reglamento (UE) 2022/2554 (DORA).

Parlamento Europeo y del Consejo de la UE. (2024). Reglamento (UE) 2024/2847 (CRA).

Para facilitar la consulta, se incluyen a continuación las URLs de acceso a los principales informes y documentos institucionales referenciados a lo largo del estudio:

Everstream Analytics 2026 Risk Report: https://www.everstream.ai/risk-center/supply-chain-risk-reports/2026-annual-risk-report/

ENISA Threat Landscape 2025: https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape

IBM Cost of a Data Breach 2025: https://www.ibm.com/reports/data-breach

ISC2 Cybersecurity Workforce Study 2024: https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study

NIST SP 800-207 (Zero Trust): https://doi.org/10.6028/NIST.SP.800-207

NIST SP 800-161r1 (Supply Chain Risk): https://doi.org/10.6028/NIST.SP.800-161r1

Verizon DBIR 2025: https://www.verizon.com/business/resources/reports/dbir/

WEF Global Risks Report 2024: https://www.weforum.org/reports/global-risks-report-2024/

Black Kite 2025 Supply Chain Vulnerability Report: https://content.blackkite.com/ebook/2025-supply-chain-vulnerability-report

Directiva NIS2 (EUR-Lex): https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32022L2555

Cyber Resilience Act (EUR-Lex): https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32024R2847

Esquema Nacional de Seguridad (BOE): https://www.boe.es/eli/es/rd/2022/05/03/311

SOCRadar Top Supply Chain Attacks 2025: https://socradar.io/blog/top-10-supply-chain-attacks-2025

NTT DATA Ciberataques España 2026: https://es.nttdata.com/newsfolder/espana-ciberataques-industria-en-riesgo-2025

Patrocinado por:

Centro Español de Logística

ZLC | MIT GLOBAL SCALE NETWORK

gmv INNOVATING SOLUTIONS