Telefónica Tech

NextDefense

Protección de la cadena de suministro

Claves para la ciberresiliencia

Estrategias de ciberseguridad efectivas para la gestión de riesgos de terceros.
Soluciones para anticiparse a amenazas y proteger tus activos críticos.

Resumen

En el último año, el 60% de las empresas ha reportado una brecha de seguridad en la cadena de suministro, exponiendo a las organizaciones a riesgos invisibles. Este documento aborda un aspecto crítico e ignorado: la protección frente a ciberamenazas de terceras y cuartas partes.

La digitalización de procesos y la expansión de operaciones de empresas y organizaciones amplían las superficies de ataque, incrementando riesgos y vulnerabilidades. Si no se gestionan adecuadamente, proveedores remotos, subcontratistas y componentes digitales comunes se convierten en vectores de riesgo. Para enfrentar este desafío, presentamos el enfoque FPRM (Fourth-Party Risk Management), que anticipa efectos en cascada de actores indirectos, integrándose en estrategias de ciberseguridad para proteger cada nivel de la cadena de suministro.

Este documento propone un marco de acción práctico que combina visibilidad, trazabilidad y colaboración. Incluye prácticas como auditorías extendidas, simulacros sectoriales, monitorización continua y cláusulas contractuales bajo normativas internacionales recientes, incluidas NIS2, DORA y el Cyber Resilience Act, que redefinen los estándares de ciberseguridad a nivel global.

Además, exploramos soluciones como **Third-Party Risks** de Telefónica Tech, que permiten evaluar y mitigar riesgos de forma automatizada y basada en datos. Este enfoque integral conecta tecnología avanzada, procesos sólidos y una cultura organizacional comprometida.

En este documento encontrarás las claves para proteger tus activos críticos, reducir tu exposición a brechas y construir una cadena de suministro resiliente preparada para los desafíos digitales actuales.

CONTENIDO

1. INTRODUCCIÓN 4
2. PANORAMA ACTUAL: AMENAZAS, IMPACTOS Y TENDENCIAS 5
3. DE LA TEORÍA A LA PRÁCTICA: CIBERSEGURIDAD EN LA CADENA DE SUMINISTRO 7
4. NORMATIVAS QUE DEFINEN EL NUEVO MARCO DE CUMPLIMIENTO 9
5. SOLUCIONES Y MEJORES PRÁCTICAS PARA UNA DEFENSA EFICAZ 11
6. ESTRATEGIA RECOMENDADA: ENFOQUE INTEGRAL 12
7. EL CAMINO HACIA LA CIBERRESILIENCIA 13

1. Introducción

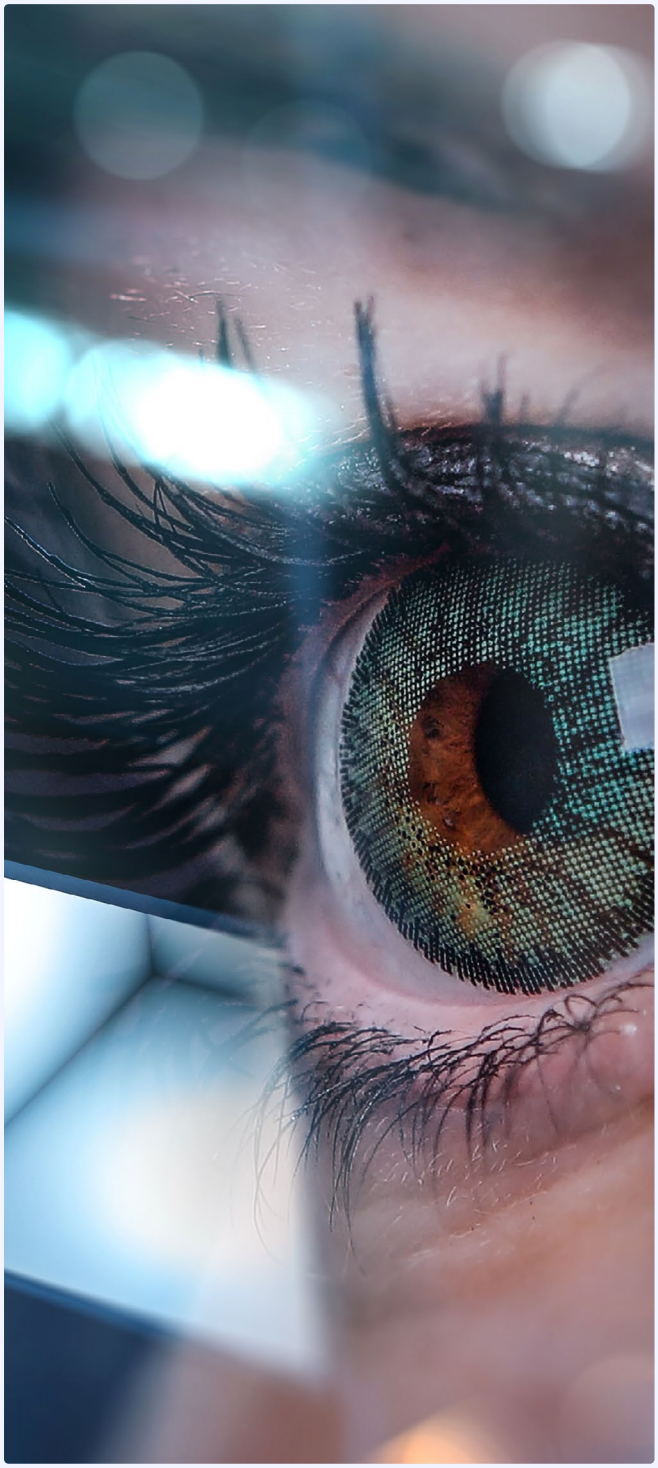
La ciberresiliencia ya no es opcional. Es indispensable para la continuidad de los negocios en un mundo interconectado.

La digitalización masiva de procesos críticos, industriales y operacionales ha transformado el panorama de las organizaciones modernas. Este cambio ha permitido avances en eficiencia, productividad y conectividad, pero también ha ampliado las superficies de ataque, generando riesgos que trascienden los límites físicos y digitales.

Las amenazas ya no se limitan al entorno interno de las empresas. Se extienden a un ecosistema digital de terceros y actores externos que pueden introducir vulnerabilidades. En este contexto, la ciberseguridad se convierte en un pilar estratégico para garantizar resiliencia operativa, cumplimiento normativo y confianza entre socios, clientes y ciudadanos.

Las cadenas de suministro son vulnerables a ataques sofisticados por su carácter distribuido y transnacional. Este documento analiza los riesgos actuales y ofrece herramientas y estrategias para proteger activos sensibles, anticiparse a los riesgos y fomentar una cultura de ciberresiliencia.

Te invitamos a explorar **cómo proteger tus activos** sensibles, anticiparte a los **riesgos de terceras y cuartas partes** y desarrollar una cultura de ciberresiliencia con **estrategias que fortalecen tus defensas digitales** y fomentan la colaboración entre todos los actores involucrados.



2. Panorama actual: amenazas, impactos y tendencias

Las amenazas digitales son una realidad diaria que evoluciona más rápido que las defensas convencionales.

El entorno de amenazas actual se caracteriza por ataques más sofisticados, la explotación de nuevas tecnologías y un ecosistema digital frágil.

Las organizaciones enfrentan riesgos en las siguientes áreas:

AMENAZAS TECNOLÓGICAS

- **Ataques por vulnerabilidades zero-day:** brechas desconocidas que se explotan antes de que se desarrollen parches.
- **Malware adaptativo y polimórfico:** programas de software maliciosos que cambian para evadir defensas tradicionales.
- **Exfiltración de datos a través de interfaces API y dispositivos IoT:** acceso no autorizado a información sensible a través de puntos de integración mal protegidos.
- **Ataques a modelos de IA (data poisoning, inferencia, robo de modelos):** vulnerabilidades que afectan la seguridad de los sistemas de IA e IA Generativa.

AMENAZAS HUMANAS

- **Phishing hiperrealista impulsado por IA:** mensajes fraudulentos creados con IA que imitan a remitentes legítimos.
- **Deepfakes y robo de identidad digital:** creación de contenido multimedia falso para suplantar identidades y manipular.
- **Proveedores vulnerables o comprometidos:** actores con bajo nivel de madurez en ciberseguridad que se convierten en puertas traseras hacia organizaciones mejor protegidas.

AMENAZAS REGULATORIAS Y SISTÉMICAS

- **Riesgos del uso de software de terceros:** integración de herramientas que crean nuevas superficies de ataque si no son auditadas adecuadamente.
- **Ciberamenazas sistémicas y efectos en cascada:** ataques que se originan en un eslabón remoto de la cadena y escalan rápidamente al resto del ecosistema.
- **Impactos regulatorios y geopolíticos:** operar globalmente añade complejidad legal y expone a restricciones comerciales o tensiones políticas.

Estos riesgos podrían afectar la disponibilidad, integridad y confidencialidad de los servicios esenciales, impactando a las empresas y la estabilidad económica y social.

Gestión de Riesgos de Cuartas Partes (FPRM)

En un ecosistema digital interconectado los riesgos no terminan en tus proveedores directos, se extienden a actores fuera de tu control.

Las amenazas mencionadas no solo impactan a las organizaciones. Su complejidad y evolución pueden propagarse a través de actores indirectos en las cadenas de suministro. Aquí, el **efecto en cascada** se convierte en un peligro: una vulnerabilidad en un proveedor remoto o subcontratista puede escalar rápidamente, comprometiendo la estabilidad de múltiples organizaciones conectadas.

La **Gestión de Riesgos de Cuartas Partes (FPRM)** surge como respuesta crítica para abordar amenazas que, aunque inicialmente parecen periféricas, pueden causar interrupciones significativas. Este enfoque se centra en identificar, evaluar y mitigar los riesgos de los proveedores de tus proveedores, actores que operan fuera de tu control directo pero que son esenciales en tu ecosistema digital.

¿Por qué gestionar el riesgo de las cuartas partes?

En un contexto de creciente conectividad e interdependencia, es imperativo que las organizaciones adopten una visión proactiva y ampliada de la gestión de riesgos. Esto implica auditar a los proveedores directos, mapear las relaciones en la cadena, evaluar continuamente su postura de seguridad y definir controles claros.

Las empresas quedan expuestas a vulnerabilidades invisibles que pueden desatar efectos en cadena devastadores si no abordan estos riesgos integralmente. La prevención y supervisión activa son estratégicas para garantizar la resiliencia operativa y la confianza.

Las organizaciones deben entender que **el riesgo no termina en sus proveedores directos.** Identificar, evaluar y mitigar los riesgos que plantean las cuartas partes es esencial para construir resiliencia operativa en un ecosistema digital interdependiente.

En la siguiente sección abordamos **cómo trasladar este enfoque a la práctica** mediante estrategias de ciberseguridad orientadas específicamente a proteger la cadena de suministro en todos sus niveles.

3. De la teoría a la práctica: Ciberseguridad en la cadena de suministro

La seguridad de tu cadena de suministro depende de su eslabón más débil. La visibilidad, control y colaboración son esenciales para protegerla.

Las amenazas no se limitan a proveedores directos. Cada eslabón indirecto, las cuartas y enésimas partes, representa un punto de entrada potencial para ataques sistémicos. Los principales retos son:

- **FALTA DE VISIBILIDAD SOBRE LA RED DE TERCEROS:** muchas organizaciones desconocen los proveedores con los que interactúan sus socios directos, lo que limita su capacidad de evaluación y supervisión.
- **AUSENCIA DE TRAZABILIDAD Y MAPEO DEL ECOSISTEMA DIGITAL:** sin inventarios claros de dependencias tecnológicas y relacionales, es inviable identificar los vectores de riesgo indirectos.
- **DIFICULTAD PARA AUDITAR O APLICAR CONTROLES EN ENTORNOS AJENOS:** la tercerización y subcontratación difuminan los límites de responsabilidad y reducen la eficacia de las medidas preventivas.
- **DIVERSIDAD DE MADUREZ Y CUMPLIMIENTO EN LA CADENA:** la heterogeneidad de capacidades técnicas y culturales en ciberseguridad impide una defensa homogénea.
- **RIESGOS REGULATORIOS Y GEOPOLÍTICOS:** operar con proveedores internacionales añade complejidad legal y expone a tensiones políticas, restricciones comerciales o legislación contradictoria.
- **FALTA DE ESTÁNDARES COMUNES Y MECANISMOS DE CERTIFICACIÓN DE PROVEEDORES:** la ausencia de marcos universales para evaluar el riesgo de terceros dificulta las comparativas y decisiones informadas.
- **TIEMPO DE RESPUESTA ANTE INCIDENTES DE TERCEROS:** sin canales de comunicación definidos o visibilidad sobre los sistemas de proveedores, lo que retrasa la detección y contención.

Caso práctico

Una empresa farmacéutica ficticia sufrió un impacto crítico debido a un ataque en su cadena de suministro. El ataque comenzó con una pequeña empresa de transporte subcontratada que gestionaba el traslado de vacunas. Los atacantes explotaron una vulnerabilidad en el software de logística de esa empresa, accediendo a datos sensibles sobre rutas y almacenes.

Los atacantes interceptaron un envío crítico y alteraron datos logísticos para retrasar la distribución en regiones clave. Como resultado, esta empresa sufrió pérdidas financieras, daños a su reputación y sanciones regulatorias por incumplimientos en la entrega de suministros médicos. La empresa no había auditado la ciberseguridad de este pequeño proveedor, subestimando su rol en la cadena.

Para mitigar futuros incidentes, la empresa adoptó múltiples medidas preventivas:

- **Se implementaron auditorías periódicas de ciberseguridad** a todos los proveedores, incluidos los de menor relevancia operativa.
- **Desarrollaron simulacros de respuesta ante incidentes** específicos para el sector logístico, involucrando a proveedores directos e indirectos.
- **Adoptaron tecnologías de monitorización continua**, como software que mapea en tiempo real la seguridad de la cadena de suministro.
- **Formalizaron acuerdos de nivel de servicio (SLA)** con cláusulas estrictas sobre ciberseguridad, estableciendo responsabilidades claras en caso de incidentes.

Estas acciones reforzaron su seguridad y aumentaron la confianza de sus socios, proveedores y clientes. Este caso resalta la necesidad de una estrategia robusta para gestionar el riesgo en toda la cadena de suministro, desde los actores principales hasta los eslabones más pequeños.

Gestión integral del riesgo. La lección principal de esta historia ficticia es que la gestión del riesgo debe incluir evaluaciones de 'onboarding' rigurosas, monitorización continua de la seguridad de proveedores, contratos con requisitos de ciberseguridad claros, y ejercicios conjuntos de respuesta ante incidentes. Sin estas medidas, incluso los actores más protegidos pueden volverse vulnerables a través de terceros.

4. Normativas que definen el nuevo marco de cumplimiento

La regulación es clave para construir confianza digital, anticiparse al riesgo y fortalecer la resiliencia organizacional.

La respuesta regulatoria se ha acelerado internacionalmente, impulsando marcos que integran la ciberseguridad en el ciclo de vida digital.

Ejemplos destacados incluyen:

- **Directiva NIS2:** Extiende los requisitos de resiliencia a proveedores esenciales y exige auditorías sobre terceros.

  Ejemplo: *Una empresa energética europea que subcontrata servicios críticos a una firma de TI debe implementar evaluaciones regulares de ciberseguridad y notificar incidentes dentro de plazos más estrictos, reduciendo el riesgo de interrupciones generalizadas.*

- **Reglamento DORA (Digital Operational Resilience Act)** establece medidas como pruebas de resiliencia y gestión de riesgos TIC, orientadas al sector financiero europeo.

  Ejemplo: *Bancos que integran simulacros de ataques cibernéticos en sus operaciones para garantizar la continuidad del servicio frente a brechas en proveedores tecnológicos.*

- **Reglamento de Inteligencia Artificial, AI Act (UE):** Clasifica sistemas de inteligencia artificial por niveles de riesgo y establece requisitos.

  Ejemplo: *Un proveedor de soluciones de reconocimiento facial debe cumplir requisitos de trazabilidad y supervisión humana para operar en la Unión Europea.*

- **Reglamento CRA (Cyber Resilience Act):** Aplica a productos con elementos digitales, exigiendo diseño seguro desde el origen y actualizaciones de seguridad continuas.

  Ejemplo: *Fabricantes de dispositivos IoT en Europa deben proporcionar parches de seguridad durante el ciclo de vida, reduciendo vulnerabilidades.*

- **Ley de Ciberseguridad de China** impone revisiones de seguridad y almacenamiento de datos en el país.

  Ejemplo: *Empresas internacionales en China han ajustado sus políticas de datos, incluyendo restricciones para transferir información fuera del país.*

- **Executive Order 14028 (EE. UU.):** Refuerza requisitos de ciberseguridad para proveedores del gobierno federal, promoviendo los SBOM (Software Bill of Materials).

  Ejemplo: *Contratistas de software para el gobierno de EE. UU. deben proporcionar listas detalladas de componentes de software para garantizar el control y la ausencia de vulnerabilidades.*

ESTÁNDARES INTERNACIONALES

- **ISO 27001:** Gestión de la seguridad de la información.

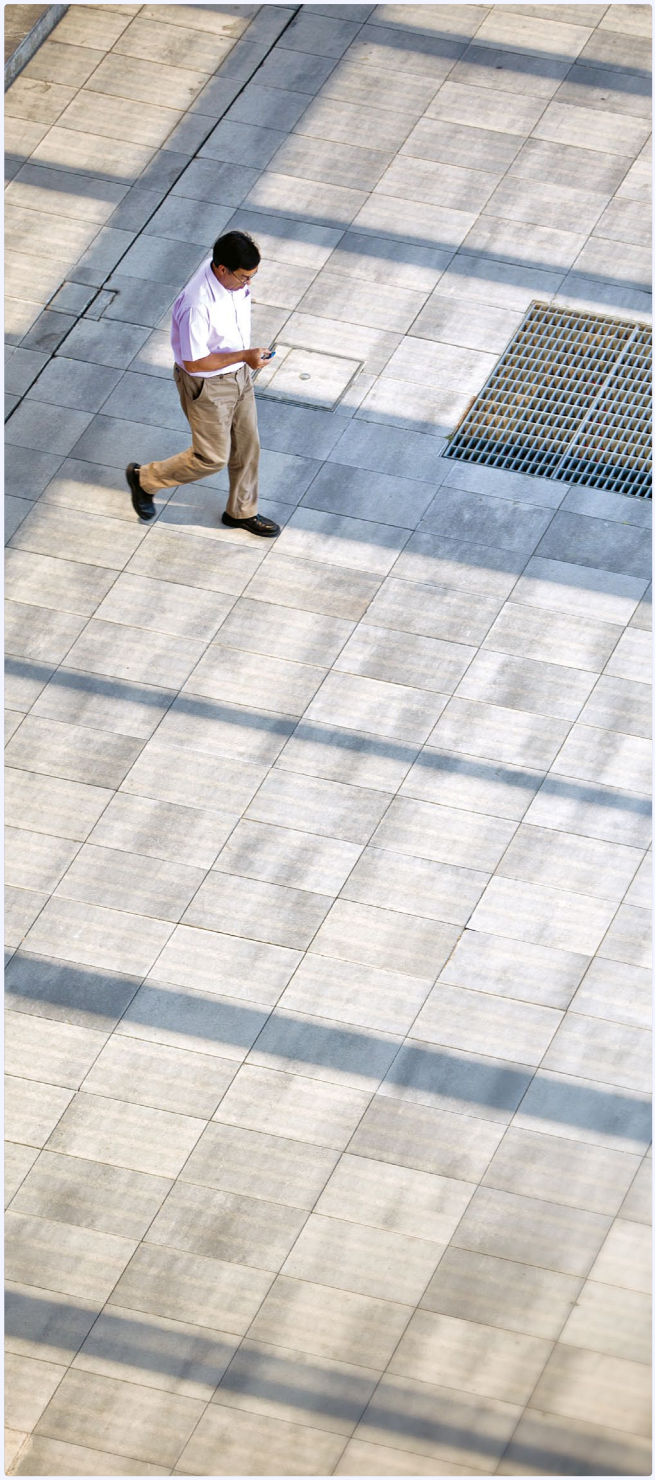
  Ejemplo: *Una empresa multinacional adopta este estándar para estructurar y documentar sus políticas de seguridad y facilitar auditorías externas.*

- **ISO 22301:** Continuidad del negocio.

  Ejemplo: *Un proveedor farmacéutico usa ISO 22301 para minimizar interrupciones en la producción de medicamentos esenciales tras un ciberataque.*

- **NIST CSF:** Marco para identificar, proteger, detectar, responder y recuperar.

  Ejemplo: *Una compañía de telecomunicaciones estadounidense implementa NIST CSF para fortalecer la gobernanza de seguridad en sus infraestructuras críticas.*



Cumplimiento normativo y privacidad de datos

El cumplimiento normativo y la privacidad de datos son pilares en la gestión de riesgos modernos, especialmente con leyes y regulaciones en evolución. En Telefónica Tech ayudamos a las empresas a adoptar un enfoque integral que garantice el alineamiento con normativas clave como el RGPD y otras legislaciones internacionales, minimizando riesgos legales y reputacionales.

Nuestras soluciones permiten a las empresas implementar estándares de seguridad que cumplen con las exigencias regulatorias y refuerzan la confianza de clientes, socios y partes. Nuestro enfoque proactivo incluye la trazabilidad de datos, protección de información sensible y adaptación a nuevos requisitos regulatorios, garantizando la resiliencia y sostenibilidad operativa de las organizaciones.

No deben verse estas normativas como una carga burocrática, sino como una oportunidad estratégica para mejorar la madurez cibernética de las organizaciones. Adoptarlas proactivamente permite alinear la seguridad con la innovación, minimizar riesgos legales y fortalecer la confianza de clientes, reguladores y socios.

5. Soluciones y mejores prácticas para una defensa eficaz

Una defensa eficaz no se construye con tecnología aislada, sino con la sinergia entre herramientas inteligentes, procesos sólidos y personas comprometidas.

Una estrategia de ciberseguridad efectiva se basa en tres pilares: tecnología, procesos y personas. Deben integrarse de forma coordinada para ofrecer una defensa holística y resiliente.

TECNOLOGÍA

- Arquitectura Zero Trust: implementa el principio de "nunca confiar, siempre verificar", restringiendo el acceso solo a usuarios autenticados y autorizados en cada punto de la red.
- Segmentación de red: aísla entornos IT, OT y de terceros para contener amenazas y minimizar el movimiento lateral.
- Herramientas como Clean Email (protección contra suplantación y emails maliciosos) y Security Edge (control y visibilidad del acceso remoto y en la nube).
- Sistemas de detección y respuesta (EDR/XDR): monitoriza endpoints y redes con respuesta automática.
- Plataformas de Threat Intelligence: anticipa amenazas mediante información contextualizada y accionable.

PROCESOS

- Definir políticas y procedimientos: establece protocolos claros para gestionar accesos, actualizaciones, backup, respuesta a incidentes y evaluación de proveedores.
- Gestión continua del riesgo de terceros: realiza evaluaciones regulares, seguimiento de compromisos y auditorías a proveedores clave.
- DevSecOps seguros: integra la seguridad desde el diseño en los ciclos de desarrollo de software.
- MLOps seguros: aplica principios de seguridad en el desarrollo, despliegue y operación de modelos de aprendizaje automático.
- MLOps (Machine Learning Operations) asegura que los modelos de IA se gestionen de manera confiable, protegidos frente a riesgos como la manipulación de datos, la fuga de modelos y el uso indebido de algoritmos.
- Simulacros de ciberincidentes: ensaya escenarios críticos para validar la capacidad de respuesta de todos los actores.

PERSONAS

- Concienciación y formación continua: capacita a empleados y proveedores sobre buenas prácticas, nuevas amenazas y su papel en la defensa.
- Gobernanza clara: define responsabilidades, comités de seguridad y líneas de escalado ante incidentes.
- Cultura de seguridad: promueve en todos los niveles de la organización comportamientos responsables y proactivos frente al riesgo digital.

Cuando estos tres componentes se alinean, las organizaciones mejoran su postura de seguridad y fortalecen su capacidad para resistir, recuperarse y adaptarse ante ciberamenazas.

El objetivo es consolidar una postura de seguridad resiliente mediante un enfoque coordinado que integre tecnología avanzada, procesos operativos robustos y una cultura organizacional orientada a la prevención, detección y respuesta ante amenazas.

6. Estrategia recomendada: enfoque integral

Una estrategia aislada es vulnerable. Solo una visión sistémica permite resistir las amenazas presentes y futuras.

Abordar la ciberseguridad de infraestructuras y sus cadenas de suministro requiere una estrategia global que contemple la interdependencia de riesgos, la dinámica de amenazas y la diversidad de actores. Una aproximación holística puede llenar los vacíos que las soluciones individuales no abordan, priorizando recursos y acelerando la respuesta ante incidentes.

Elementos clave de una estrategia integral

1. Gobernanza clara y efectiva: Adopta marcos como GRC (Gobernanza, Riesgo y Cumplimiento) para estructurar responsabilidades y alinear políticas de seguridad con los objetivos de negocio. Utiliza herramientas para mapear riesgos, automatizar controles y agilizar la toma de decisiones.
2. Colaboración internacional: Participa en iniciativas multilaterales y foros de cooperación para abordar amenazas globales. Adapta procesos internos a normativas globales como NIS2, CRA o DORA para facilitar el cumplimiento en varios mercados.
3. Alianzas público-privadas: Establece redes de colaboración que compartan inteligencia y recursos para prevenir y mitigar ciberamenazas. Por ejemplo, integrarse en plataformas de Threat Intelligence que ofrezcan alertas tempranas.
4. Formación continua: Invierte en capacitación y promueve una cultura de ciberseguridad en toda la organización para minimizar riesgos humanos. Realiza simulaciones periódicas para medir y mejorar la preparación ante ciberincidentes.

Una estrategia integral no es una suma de soluciones desconectadas. Es un marco coordinado que anticipa riesgos, optimiza recursos y fortalece la capacidad de recuperación ante cualquier ataque. Quienes adopten esta visión estarán mejor preparados para liderar y resistir en el entorno digital.

7. El camino hacia la ciberresiliencia

La prevención no es un gasto, es una inversión estratégica. Estar preparado hoy evita una crisis mañana.

Acciones clave

1. Diagnosticar el estado actual de ciberseguridad: Realiza auditorías técnicas y simulaciones para evaluar vulnerabilidades en la organización y la cadena de suministro.
2. Fortalecer la gobernanza: Establece políticas de seguridad, roles definidos y flujos de decisión alineados con objetivos estratégicos.
3. Desarrollar un plan de continuidad y recuperación: Implementa estrategias para mantener operaciones críticas en contingencias.
4. Formalizar acuerdos de ciberseguridad con proveedores: Incluye cláusulas de seguridad en contratos, auditorías y gestión de incidentes.
5. Promover una cultura de ciberresiliencia: Capacita a empleados y socios en buenas prácticas y conciencia sobre amenazas digitales.
6. Colaborar con redes sectoriales y plataformas de inteligencia: Participa en iniciativas que compartan información sobre nuevas amenazas.
7. Adoptar tecnologías disruptivas para confianza automatizada: Incorpora blockchain y contratos inteligentes para reforzar la trazabilidad y transparencia en la cadena de suministro. Estas tecnologías automatizan procesos clave, reduciendo riesgos de manipulación o errores humanos, y garantizan la integridad de los datos compartidos.

Servicios como **Third-Party Risks** de Telefónica Tech pueden complementar estos esfuerzos. Este servicio permite la monitorización continua del nivel de ciberseguridad en tu cadena de suministro de forma no intrusiva y automatizada.

Al integrar soluciones como esta, puedes identificar y priorizar los riesgos más críticos, optimizando recursos y fortaleciendo la seguridad.

El momento de actuar

La ciberresiliencia no se logra con promesas, sino con visión, compromiso y ejecución sostenida.

En Telefónica Tech sabemos que la ciberresiliencia de las infraestructuras y sus cadenas de suministro es clave para el éxito de cualquier organización.

Los ecosistemas empresariales están cada vez más interconectados, lo que genera oportunidades y también nuevos riesgos.

La dependencia de terceros sigue siendo un vector de riesgo crítico y multifacético. Según Bitsight, el 59% de las empresas ha reportado una brecha de datos causada por un tercero. Además, recuerda que "existen 'pilares ocultos' en la cadena de suministro, con pocos proveedores concentrando gran parte del riesgo sistémico."

Este riesgo se extiende a amenazas específicas como el ransomware, que se ha incrementado un 25% en el último año, intensificando sus ataques contra empresas más pequeñas, según el estudio State of the Underground (2025).

Por eso, en Telefónica Tech ofrecemos capacidades para protegerte frente a nuevas amenazas. Nuestras soluciones como **Third-Party Risks,** respaldadas por nuestro ecosistema de partners y los servicios profesionales de nuestro DOC global, te permiten:

- **Monitorizar** continuamente la seguridad de sus proveedores.
- **Medir y mitigar** los riesgos en la cadena de suministro mediante datos.
- **Cuantificar y comunicar** riesgos en términos accesibles para todos los niveles organizativos.

Además, la integración de tecnologías como blockchain puede ser clave para aumentar la confianza entre actores y garantizar la seguridad del ecosistema digital.

En Telefónica Tech te ayudamos a evaluar tu seguridad, identificar vulnerabilidades y aplicar soluciones avanzadas que impulsen tu resiliencia operativa y confianza digital.

Nuestro equipo de expertos trabajará contigo en una estrategia integral adaptada a tus necesidades. Juntos protegeremos tus activos, reforzaremos la confianza de tus clientes, proveedores y socios, y aseguraremos la sostenibilidad y competitividad de tu negocio. El momento de actuar es ahora.

Telefónica Tech