**Documento de trabajo de ICC**

# Protección de la ciberseguridad de las infraestructuras críticas y sus cadenas de suministro

# Resumen ejecutivo

Proteger la ciberseguridad de las infraestructuras críticas y sus cadenas de suministro es crucial por la sencilla razón de que estos sistemas impulsan nuestra vida cotidiana, desde la electricidad y el agua hasta la sanidad y el transporte. Un incidente cibernético que interrumpa el funcionamiento de estos servicios vitales puede provocar un caos generalizado, poner vidas en peligro y paralizar las economías. A medida que las ciberamenazas se vuelven cada vez más sofisticadas y omnipresentes, garantizar la resiliencia y la seguridad de estos sistemas críticos no es sólo una necesidad tecnológica, sino una salvaguarda fundamental para el bienestar y la continuidad de la vida moderna.

**Este documento explora las complejidades de la protección de estos sistemas** derivadas de múltiples factores:

- Muchos de estos servicios no fueron diseñados originalmente como servicios esenciales, lo que da lugar a tecnologías obsoletas y vulnerabilidades estructurales. La integración de componentes digitales con sistemas físicos amplifica los riesgos debido a las vulnerabilidades combinadas de ambos ámbitos, sobre todo teniendo en cuenta la rápida difusión de tecnologías nuevas y emergentes.
- La creciente complejidad e interdependencia de las cadenas de suministro amplían la superficie de ataque, por lo que resulta esencial abordar los riesgos de terceros. Además, la interdependencia de estos servicios con infraestructuras no críticas complica el establecimiento de límites claros y la inversión adecuada.
- Los limitados recursos y presupuestos de los sectores público y privado también dificultan la aplicación de medidas de seguridad sólidas. Las prácticas sólidas de seguridad, la colaboración público-privada y la cooperación internacional son cruciales para salvaguardar estos sistemas vitales, garantizar la estabilidad económica mundial y mantener la confianza en la economía digital.
- La naturaleza distribuida de las capacidades digitales exige una cooperación mundial, pero faltan consenso e incentivos internacionales. La definición de infraestructura crítica varía a escala global, lo que complica la cooperación y la coordinación internacionales. Los impactos transfronterizos y las dependencias compartidas requieren esfuerzos globales armonizados y normas alineadas, así como marcos sectoriales específicos para mitigar eficazmente los riesgos..

**A fin de proporcionar una taxonomía y recomendaciones estratégicas para abordar estos retos, el documento analiza el estado actual de la ciberseguridad para las infraestructuras críticas y sus cadenas de suministro**, evalúa los marcos, políticas y tecnologías existentes, valorando sus puntos fuertes y débiles e identificando las mejores prácticas, así como las áreas que necesitan mejoras..

**El documento demuestra cómo, en respuesta a las amenazas cibernéticas, el sector privado refuerza la resiliencia y la recuperación** mediante la adopción de medidas de seguridad integrales, incluyendo la adopción de los principios de ciberseguridad por diseño, el mantenimiento de inventarios de activos robustos, el desarrollo de planes de respuesta a incidentes, la implementación de copias de seguridad de datos, asegurando sistemas actualizados con los últimos parches de seguridad y arquitecturas zero-trust, así como una política de cadena de suministro sólida. Presenta las mejores prácticas y las normativas existentes en el sector que pueden ampliarse y adoptarse de forma más general.

Al mismo tiempo, aunque la inversión empresarial en prevención y capacidades defensivas es esencial, el sector privado por sí solo es incapaz de disuadir, prevenir o protegerse a sí mismo (y a las comunidades que ayuda a mantener) de los efectos destructivos de los ciberataques. **La ciberseguridad es una responsabilidad compartida entre los sectores público y privado, y ambos deben trabajar juntos para mitigar los riesgos y frenar las ciberamenazas**. Esto es aún más importante en el caso de las infraestructuras críticas, donde las funciones y responsabilidades de los agentes de los sectores público y privado están estrechamente entrelazadas. **Este documento aboga por una relación estrecha, continua y conjunta entre los proveedores de infraestructuras críticas y los gobiernos para garantizar respuestas eficaces a las ciberamenazas**. Ofrece recomendaciones concretas para los responsables políticos en contextos tanto nacionales como internacionales, así como sugerencias para crear asociaciones público-privadas eficaces.

# Índice



# Introducción

Aunque las jurisdicciones de todo el mundo tienen diferentes puntos de vista sobre lo que considera específicamente dentro de esta designación, las infraestructuras críticas se refieren en general a los sistemas y activos fundamentales, tanto físicos como virtuales, que son indispensables para el funcionamiento de una sociedad, su economía y sus servicios esenciales. Tradicionalmente, las infraestructuras críticas se consideran elementos estratégicos, instalaciones, equipos, redes o sistemas, o parte de ellos, que no pueden sustituirse para prestar un *servicio esencial*. Estas infraestructuras se consideran cruciales para el bienestar y para preservar el orden público y la seguridad de las naciones, por lo que su interrupción podría tener consecuencias importantes. No pueden reproducirse ni sustituirse fácilmente a corto plazo, por lo que se considera que necesitan una protección física y digital especial. Puede tratarse de sectores como la energía, el agua, el transporte, las finanzas o las comunicaciones. La mayoría de estos sistemas dependen en gran medida de redes informáticas, sistemas de control y tecnologías digitales, lo que los hace susceptibles a las ciberamenazas.

El concepto de *servicios esenciales* es de especial relevancia a la hora de designar una infraestructura como "crítica", y se refiere al mantenimiento de las funciones vitales de la sociedad, las actividades económicas, la salud y seguridad públicas o el medio ambiente. Esto es tanto más importante cuando estos servicios, su desarrollo o su prestación se vuelven cada vez más digitales. Para garantizar la eficacia de las medidas de protección y la seguridad jurídica, este concepto suele estar vinculado a una lista específica de sectores considerados esenciales por los responsables públicos.[1]

Garantizar la confianza en la economía digital requiere la protección de la disponibilidad, integridad y confidencialidad de estas infraestructuras y servicios más esenciales para asegurar la resiliencia. La seguridad digital y física van de la mano para consolidar la resiliencia operativa de las organizaciones y los servicios esenciales que prestan. Cualquier fallo en la seguridad digital o física puede provocar un incidente grave en la interrupción de la prestación de servicios y la reputación de la organización. Los esfuerzos deben centrarse en mejorar tanto la seguridad digital como la física de los servicios y aumentar la resiliencia de los activos críticos frente a sucesos naturales, accidentales o intencionados. Un elemento central de estos esfuerzos es el desarrollo de un marco de gestión de riesgos adecuado y sólido, desde la identificación de las fuentes de riesgo hasta la comunicación de los incidentes a las partes interesadas.

**El objetivo de este documento es abordar las medidas de ciberresiliencia,** incluidos los mecanismos de colaboración, las medidas voluntarias del sector privado y, en caso necesario, el equilibrio entre la regulación y la viabilidad sostenible de los controles, para la protección de las infraestructuras críticas y los servicios esenciales, es decir, la capacidad de una entidad crítica para prevenir, proteger, responder, resistir, mitigar, absorber, adaptarse y recuperarse en caso de incidente cibernético. Aunque las medidas de protección digital y física deben considerarse de forma sincronizada y cada vez más coordinada, este documento se centra únicamente en el componente digital. Esto se entiende sin perjuicio de la necesidad de considerar otros fenómenos naturales, errores humanos o errores de configuración fuera del ámbito de este documento a la hora de proteger infraestructuras críticas o servicios esenciales.

1 EE.UU.: www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors Europa: www.digital-strategy.ec.europa.eu/en/policies/nis2-directive; Lista de servicios esenciales: www.eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202302450

Aunque la inversión empresarial en prevención y capacidades defensivas es esencial, el sector privado por sí solo es incapaz de disuadir, prevenir o protegerse adecuadamente a sí mismo (y a las comunidades que ayuda a mantener) de los efectos destructivos de los ciberataques.

**La ciberseguridad es una responsabilidad compartida entre los sectores público y privado, y ambos deben colaborar para mitigar los riesgos y frenar las ciberamenazas.**

Los gobiernos son los principales responsables de proteger a sus ciudadanos, a la sociedad civil y a las empresas de las amenazas extranjeras y nacionales, de estado y no afiliadas, con objetivos tanto políticos como delictivos, lo que también se aplica al ciberespacio. Una acción decidida por parte de los gobiernos para frenar las ciberamenazas y una amplia colaboración entre las múltiples partes interesadas contribuirán a reforzar la confianza económica, evitar interrupciones en el comercio mundial y garantizar un entorno cibernético más seguro en el que las empresas y las comunidades puedan prosperar. Tal y como se expone en el documento ICC Cybersecurity Issue Brief #2, la mejora de la cooperación entre las partes interesadas para luchar contra la ciberdelincuencia y la aplicación de marcos para un comportamiento de estado responsable son esenciales para reducir los ciberataques y aumentar así la seguridad.[2]

**Este documento pretende abordar de forma exhaustiva los múltiples retos** que rodean la protección de las infraestructuras críticas y los servicios esenciales ante la evolución de las ciberamenazas. Mediante el análisis de diversas perspectivas sobre la definición de infraestructura crítica y la identificación de los diversos actores, motivaciones e impactos de las ciberamenazas, pretendemos subrayar la urgencia de un enfoque armonizado. Además, al evaluar el estado actual de los esfuerzos de protección y destacar las áreas susceptibles de mejora, **este documento aboga por un enfoque coordinado que incluya la participación del sector privado, mejoras en políticas públicas, cooperación internacional y el fortalecimiento de la colaboración público-privada**.

En última instancia, nuestras recomendaciones pretenden reforzar la resiliencia de las infraestructuras críticas y los servicios esenciales, así como sus cadenas de suministro, salvaguardándolos frente a los ciberriesgos emergentes en un panorama global cada vez más interconectado. infrastructure and essential services, as well as their supply chains, safeguarding them against emergent cyber risks in an increasingly interconnected global landscape.

2 ICC Cybersecurity Issue Brief #2: Implementación de marcos y reglas para los estados y la cooperación internacional

# 1. Diferentes enfoques para definir las infraestructuras críticas y los servicios esenciales

Las infraestructuras críticas constituyen la columna vertebral de la funcionalidad y resiliencia del mundo. Estos sistemas y activos esenciales son la esencia de la sociedad. Las alteraciones de su seguridad y correcto funcionamiento pueden tener graves repercusiones, afectando a la seguridad pública, la estabilidad económica y la seguridad nacional. Hemos visto el impacto físico de la seguridad de las infraestructuras críticas en diversas geografías y sectores.

Un ejemplo es la respuesta de Costa Rica a ciberataques significativos contra instituciones públicas en 2022, declarando un Estado de Emergencia Nacional en el sector público, destacando la necesidad de cooperación internacional.[3] Esto llevó a la creación de un Plan General de Emergencia, mejorando los recursos y procesos administrativos para abordar el desafío. Aunque estas medidas mejoraron la respuesta a los ataques, el país reconoció la necesidad de un enfoque más integral y actualmente está en proceso de desarrollar la Estrategia Nacional de Ciberseguridad 2023-2027, con el objetivo de reforzar la gobernanza, adaptar el marco jurídico, mejorar la protección de las infraestructuras y la resiliencia nacional y fomentar la cooperación en el entorno digital. La estrategia se ajusta a los planteamientos estratégicos nacionales y ofrece orientaciones para la toma de decisiones.[4] También recomienda dar prioridad a la seguridad de las infraestructuras críticas definiendo con precisión las infraestructuras críticas nacionales, tanto en el sector público como en el privado, y esbozando los mecanismos esenciales de protección. Además, la estrategia hace hincapié en la importancia de reforzar la gestión de riesgos mediante la identificación y priorización de los activos críticos, las evaluaciones periódicas de los riesgos de ciberseguridad y la asignación de recursos para maximizar el rendimiento de la inversión en términos de beneficios económicos y sociales.

Los incidentes graves que han afectado a infraestructuras críticas han tenido importantes repercusiones negativas en todo el mundo y en múltiples sectores durante las últimas décadas.

**Algunos ejemplos ilustrativos de incidentes graves que afectan a infraestructuras críticas:**

- En Europa, los ataques a organizaciones estonias como el Parlamento, bancos, ministerios, periódicos y otros, ya en 2007 fueron una llamada de atención que ayudó al país a mejorar sus herramientas de ciberdefensa.[5] En 2008, Georgia sufrió un importante ataque de denegación de servicios distribuidos contra su infraestructura crítica, incluidos los servicios gubernamentales, el sector bancario y varios sitios web, con más del 70% de los sitios web georgianos afectados.[6] Se informó de un gran número de amenazas similares en el período 2008-2014[7]. Más recientemente se informó de una serie de ataques en Ucrania (como el *ransomware* wiper) tras el conflicto con Rusia.[8]

- En 2013, en Estados Unidos, unos piratas informáticos accedieron a la presa de Bowman Avenue, en Nueva York, y controlaron las compuertas. Se cree que plataformas petrolíferas, barcos, satélites, aviones de pasajeros y sistemas aeroportuarios y portuarios fueron vulnerables y los informes de los medios de comunicación sugirieron que se habrían producido brechas[9].

- En mayo de 2021, el ataque del *ransomware* al oleoducto de Colonial obligó a detener todas las operaciones comerciales[10].

3 Decreto Ejecutivo N° 43542-MP-MICITT 2022
4 www.micitt.go.cr/el-sector-informa/avanza-proceso-de-implementacion-de-la-estrategia-nacional-de-ciberseguridad
5 www.bbc.com/news/39655415
6 www.ccdcoe.org/uploads/2018/10/legalconsiderations_0.pdf
7 www.ccdcoe.org/uploads/2018/10/Ch08_CyberWarinPerspective_Weedon.pdf
8 www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology
9 www.industrialcybersecuritypulse.com/facilities/throwback-attack-how-the-modest-bowman-avenue-dam-became-the-target-of-iranian-hackers/
10 www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

- En América Central y del Sur, en enero de 2024, el ataque de Trigona a las operaciones de Claro causó más de una semana de interrupción de servicios[11].

Si bien la seguridad de los componentes digitales de las infraestructuras críticas que prestan servicios esenciales es clave para salvaguardar la resiliencia, **la combinación de capacidades digitales y componentes físicos**, como en Internet de las cosas (IoT) o la tecnología operativa (OT), **conlleva una explosión de nuevos riesgos potenciales derivados del efecto conjunto de la tecnología digital y las vulnerabilidades y la complejidad del mundo físico**. Un ejemplo de ello fue el caso de Stuxnet[12], mediante el cual un *malware* especializado fue capaz de perjudicar el programa nuclear iraní a través de un ataque digital para cambiar parámetros físicos en los sistemas SCADA nucleares iraníes.

Estos incidentes ponen de relieve el potencial efecto desestabilizador de un ataque contra infraestructuras críticas y subrayan la importancia de unas prácticas de seguridad sólidas y de la colaboración entre las partes interesadas para disuadir, proteger y hacer frente a las ciberamenazas.

Además, **en un mundo cada vez más interconectado, la importancia de la protección de las infraestructuras críticas trasciende las fronteras y se extiende a escala mundial**. Con dependencias compartidas y posibles repercusiones transfronterizas, una brecha en una región puede afectar a otra.

Los incidentes cibernéticos transversales que se pueden nombrar van desde el extendido Wannacry que afectó a todas las regiones del mundo[13], a diversas vulnerabilidades y ataques a la cadena de suministro de software y servicios digitales, que afectan a organizaciones de diferentes países. Un ejemplo es un incidente ocurrido en 2017, cuando el gigante del transporte marítimo Maersk, con sede en Copenhague, Dinamarca, se convirtió en víctima del ataque de *ransomware* NotPetya[14]. Maersk es una de las mayores empresas de transporte del mundo, responsable de una quinta parte del transporte marítimo mundial. Como consecuencia del ataque, las operaciones de carga de Maersk en cuatro países diferentes fueron afectados, causando retrasos e interrupciones que duraron semanas, además de costar a la empresa más de 200 millones de dólares para remediarlo. Otros ejemplos recientes son *Log4shell*[15], *SolarWinds*[16], e Ivanti[17].

**Los esfuerzos armonizados para establecer una base de referencia que proteja las infraestructuras críticas son cruciales** para fomentar la colaboración internacional, la resiliencia frente a las amenazas emergentes y garantizar la estabilidad de los sistemas interconectados que sustentan el mundo moderno a escala global. Mediante la aplicación de medidas mínimas de protección armonizadas a escala general, podemos salvaguardar estos activos fundamentales frente a diversas amenazas, como catástrofes nacionales, ciberataques y daños deliberados.

Sin embargo, las definiciones globales divergentes de infraestructuras críticas y servicios esenciales, y los requisitos contradictorios plantean retos a la cooperación y coordinación internacionales para disminuir las ciberamenazas y desarrollar soluciones eficaces de mitigación de riesgos. La desalineación puede obstaculizar la comunicación y la colaboración efectivas durante las crisis transfronterizas. Para una visión general de las distintas jurisdicciones en materia de infraestructuras críticas, véase el **Anexo I**.

> **El primer paso para llegar a un acuerdo común sobre la terminología para gestionar los riesgos de las infraestructuras críticas es la convergencia en el uso de normas internacionales reconocidas globalmente y ampliamente utilizadas.**

Por ejemplo, las normas ISO, el Marco de Riesgos Cibernéticos del NIST, el 3GPP en el caso de la infraestructura móvil, y en el caso del sector de los servicios financieros, el *Cyber Risk Institute's 'Profile*, pueden utilizarse para cumplir la normativa financiera global. La utilización de estas normas comunes ayuda a garantizar una gestión adecuada del riesgo con un alto nivel de seguridad y privacidad.

11 www.commsrisk.com/ransomware-ataque-golpea-a-claro-en-latinoamerica/
12 www.spectrum.ieee.org/la-historia-real-de-stuxnet
13 www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/
14 El ataque del ransomware NotPetya costó al gigante naviero Maersk más de 200 millones de dólares (forbes.com).
15 www.ibm.com/topics/log4shell
16 www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12?r=US&IR=T
17 www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b

Al mismo tiempo, los propietarios y operadores de infraestructuras críticas dependen de una red de suministradores para funcionar. Por lo tanto, los riesgos de la cadena de suministro y de terceros son una extensión de los servicios esenciales. La rápida expansión de la economía digital en los últimos años ha aumentado exponencialmente el número de terceros en nuestros ecosistemas. A medida que las cadenas de suministro se hacen más complejas, interdependientes e interconectadas, la exposición al riesgo también crece. La superficie de ataque aumenta, y la probabilidad de un incidente y los impactos en cascada resultantes se vuelven más difíciles de predecir, identificar y mitigar para los propietarios y operadores de infraestructuras críticas.

Por lo general, los terceros no están diseñados para hacer frente a tal criticidad, ni en términos de sus controles técnicos y operativos ni de su sostenibilidad financiera, lo que plantea el dilema de su viabilidad para servir al propósito de tales infraestructuras críticas y servicios esenciales.

La seguridad de las infraestructuras críticas es fundamental para nuestra seguridad económica mundial y la protección de la confianza en nuestra economía digital compartida. **La convergencia en las definiciones, la armonización de las normas y los marcos mundiales y unos sólidos planteamientos de gestión de riesgos de suministradores pueden contribuir a elevar el listón de la seguridad**.

# 2. Retos de la protección de infraestructuras críticas

Dada su importancia capital para el funcionamiento de las sociedades y las economías, la salvaguarda de las infraestructuras críticas se erige en el principal reto que requiere un conocimiento exhaustivo del variado panorama de las ciberamenazas.

Las amenazas digitales a las que se enfrentan las infraestructuras críticas y los servicios esenciales no son fundamentalmente diferentes de aquellas a las que se enfrenta cualquier otra capacidad, servicio o proceso digital.

**La dificultad de proteger adecuadamente las infraestructuras críticas se deriva de varios factores:**

- Muchos de estos servicios esenciales no se han desplegado como tales y han acabado adquiriendo posteriormente una relevancia esencial para la sociedad. Por tanto, no fueron concebidos con un criterio de resiliencia al nivel de relevancia que han acabado teniendo. Esto podría implicar tanto una cultura de protección por debajo de lo que es que se requieren en la actualidad y problemas de diseño que pueden afectar al modo en que pueden protegerse ahora. Un ejemplo es el propio diseño de la arquitectura de Internet, donde existen múltiples riesgos estructurales difíciles de parchear sin un cambio de raíz (estructura del DNS, protocolos descentralizados BGP, niveles insuficientes de cifrado y protección en protocolos y servicios, raíces insuficientes de confianza en las capacidades de cifrado, etc.).
- La interdependencia de los servicios esenciales y sus correspondientes infraestructuras críticas con otras infraestructuras o servicios que no están definidos como tales, hace muy difícil determinar los límites para la aplicación de criterios estrictos, inversiones adecuadas, mecanismos de colaboración, etc.
- La propia naturaleza distribuida de las capacidades digitales hace complejo poder aplicar políticas locales sin un acuerdo adecuado entre todos los países, donde se carece de incentivos o disuasiones globales para lograr un mínimo de acuerdo sobre lo que se debe proteger, por el contrario, se corre el riesgo de una escalada de agresividad entre naciones y bloques.
- La falta de conocimiento y visión global de la naturaleza de los riesgos tanto en el sector público como en el privado dificulta la consecución de normas más allá de la necesidad de proteger todas las capacidades digitales.
- La dispersión en complejas cadenas de suministro digitales también dificulta que los organismos públicos y privados se centren en criterios sencillos, lo que hace que el problema sea extenso y disperso.
- Algunos componentes de infraestructuras críticas siguen dependiendo de tecnologías anticuadas y sin soporte, lo que los hace más vulnerables a las ciberamenazas, ya que los parches de seguridad y las actualizaciones pueden no estar disponibles.
- Muchas organizaciones de infraestructuras críticas cuentan con recursos y presupuestos limitados asignados a la ciberseguridad, lo que dificulta la aplicación de medidas de seguridad sólidas y mantenerse al día de la evolución de las amenazas.

A continuación, presentamos un análisis estructurado que abarca las diversas dimensiones de estas amenazas, incluidos los actores implicados y sus motivaciones, las diversas formas de amenazas, su impacto y las complejidades a la hora de responder a dichas amenazas. Esta taxonomía sirve de base para construir estrategias de ciberseguridad eficaces y adaptadas a los intrincados retos que plantean las amenazas a las infraestructuras críticas.

## 2.1 Los actores y su motivación

Desde los Estados-nación hasta las organizaciones de ciberdelincuentes y las amenazas internas, cada actor se mueve por motivaciones distintas que pueden ir más allá de los beneficios económicos y abarcar la influencia geopolítica o los objetivos ideológicos.

**Grupos de amenazas de estado-nación o amenazas persistentes avanzadas**

Los grupos que constituyen una amenaza de tipo estado-nación suelen estar respaldados y dirigidos por sus departamentos militares, de inteligencia u otros departamentos gubernamentales. A diferencia de otros grupos mencionados en este contexto, suelen estar bien financiados y son capaces de llevar a cabo planes a largo plazo para ejecutar operaciones avanzadas a gran escala. Sus principales objetivos pueden ser la generación de ingresos, el espionaje o los ataques destructivos, y se dirigen tanto a otros países como a empresas privadas u organizaciones para obtener datos sensibles, financiación o estrategias militares[18]. Aunque todavía se discute el origen estatal de algunas de ellas, entre los ejemplos de este tipo de amenazas se afirma que se encuentran Stuxnet, mencionado anteriormente, GhostNet, del que se ha informado que ha comprometido los dispositivos de objetivos políticos, económicos y de medios de comunicación en casi 103 países[19], *Helix Kitten*, cuyos principales objetivos incluían organizaciones de los sectores aeroespacial, energético, financiero, aeroespacial, energético, financiero, hostelero y de telecomunicaciones, principalmente en Oriente Medio[20] o el más recientemente identificado *Flax Typhoon*[21], que afirmaba obtener y mantener acceso a largo plazo a las redes de las organizaciones mediante un uso mínimo de *malware*, basándose en herramientas integradas en el sistema operativo, junto con algún software normalmente benigno para permanecer silenciosamente en estas redes.

**Ataques internos**

Un ataque interno se refiere a actos maliciosos llevados a cabo por un individuo o un grupo de individuos que están asociados con la organización objetivo o son empleados de la misma[22]. Dado que los actores suelen trabajar como empleados o contratistas independientes de las infraestructuras críticas, pueden inclinarse por explotar las deficiencias de los sistemas de control de las infraestructuras críticas en lugar de atacar directamente el sistema desde el exterior. Estas personas con acceso a información privilegiada pueden ser empleados directos de la organización afectada o de un tercero que preste servicios al proveedor de servicios esenciales en su cadena de suministro, y con frecuencia están menos sujetos a controles de seguridad y habilitación. Por ejemplo, en 2020, las credenciales de dos empleados de Marriott fueron explotadas para piratear una aplicación que la empresa utilizaba como parte de sus servicios para huéspedes, exponiendo los registros de más de 5 millones de huéspedes[23].

18 https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf
19 www.infosecinstitute.com/resources/threat-intelligence/ghostnet-part-i/#gref www.wired.com/story/apt-34-iranian-hackers-critical-infrastructure-companies/
20 www.wired.com/story/apt-34-iranian-hackers-critical-infrastructure-companies/
21 www.microsoft.com/en-us/security/blog/2023/08/24/flax-typhoon-using-legitimate-software-to-quietly-access-taiwanese-organizations/
22 https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf
23 www.bbc.com/news/technology-54748843

**Grupos de hackers**

Los grupos de hackers emplean con frecuencia *malware*, *phishing* u otros métodos de pirateo para atacar infraestructuras críticas. Suelen infiltrarse e interrumpir las operaciones de infraestructuras críticas y participar en tácticas de extorsión contra gobiernos o proveedores de infraestructuras críticas[24]. Cabe mencionar que ciertos grupos de hackers, en lugar de participar directamente en ciberataques, distribuyen el *ransomware* a grupos o individuos más pequeños, formando así parte de un ecosistema más amplio y complejo de organizaciones ciberdelictivas muy especializadas, más resistentes a los desmantelamientos y la persecución. Esta tendencia ha provocado un aumento significativo del número de delincuentes que utilizan *ransomware* y de la magnitud global de los ciberdelitos en la actualidad[25]. Algunos ejemplos son el grupo Lazarus, responsable del ataque de *ransomware* WannaCry[26], REvil, conocido sobre todo por el ataque a Kaseya y supuestamente responsable del 37% de los ataques de *ransomware* en 2021[27] o Lapsus$, que realiza ataques contra empresas y organismos públicos con tácticas de ingeniería social[28].

***Hacktivistas***

A diferencia de los atacantes antes mencionados, los *hacktivistas* suelen estar más motivados por opiniones políticas o sociales que por intereses económicos. La mayoría de los *hacktivistas* implicados en ciberataques lo hacen con la intención de buscar medios alternativos para influir en la política y provocar cambios sociales. Es importante señalar que su motivación principal no es el beneficio personal. Sin embargo, este aspecto ideológico plantea un reto potencial para los proveedores de servicios de infraestructuras críticas, ya que los ataques no pueden resolverse únicamente con soluciones monetarias. Por ejemplo, Anonymous se ha atribuido la responsabilidad de inutilizar destacados sitios web rusos del gobierno, de noticias y de empresas, y de filtrar datos[29].

## 2.2 Amenazas y su impacto

Los tipos de amenazas que se ciernen sobre las infraestructuras críticas abarcan desde sofisticados programas maliciosos y ataques a la cadena de suministro hasta intrusiones físicas y ataques de denegación de servicio. Aunque los métodos utilizados por los actores maliciosos para perturbar el funcionamiento de las infraestructuras críticas son a menudo similares a las ciberamenazas en general, su potencial para causar consecuencias generalizadas y graves es significativamente más pronunciado.

Las amenazas cibernéticas a las infraestructuras críticas pueden provocar una interrupción generalizada de los servicios esenciales, afectando a grandes poblaciones. Esto puede incluir cortes de electricidad, interrupciones del transporte, problemas de abastecimiento de agua, etc., que afectan a la seguridad pública y a la economía. Pueden plantear amenazas directas a la seguridad humana. Por ejemplo, las interrupciones de un sistema de transporte podrían comprometer el control de las señales de tráfico o perturbar las operaciones ferroviarias, provocando accidentes.

Dada la naturaleza altamente interconectada e interdependiente de los sistemas de infraestructuras críticas, una interrupción en un sector puede tener efectos en cascada sobre otros. Por ejemplo, un apagón puede afectar a los sistemas sanitarios, de comunicación y de transporte. Además, dado el papel central de las infraestructuras críticas para el funcionamiento de un país, las interrupciones de estos sistemas pueden tener importantes implicaciones para la seguridad nacional.

Es importante subrayar que no sólo es importante la disponibilidad de estos servicios esenciales; en la mayoría de los casos, también se ven afectadas la confidencialidad y la integridad, lo que perjudica a la sociedad de forma similar o incluso más grave. Por ejemplo, la fuga de datos personales no puede revertirse una vez producida y perjudicará a las personas más allá de la duración real del incidente.

24 www.techcrunch.com/2019/05/12/wannacry-two-years-on/#:~:text=Two%20years%20on%2C%20the%20threat,according%20to%20los%20últimos%20datos.https://techcrunch.com/2019/05/12/wannacry-two-years-on/#:~:text=Two%20years%20on%2C%20the%20amenaza,según%20los%20últimos%20datos

25 www.ncsc.gov.uk/whitepaper/ransomware-extortion-and-the-cyber-crime-ecosystemhttps://www.ncsc.gov.uk/whitepaper/ransomware-la extorsión y el ecosistema de la ciberdelincuencia

26 www.nccgroup.com/us/the-lazarus-group-north-korean-scourge-for-plus10-years/

27 www.newsroom.ibm.com/2022-02-23-IBM-Report-Manufacturing-Felt-Brunt-of-Cyberattacks-in-2021-as-Supply-Chain-Woes-Grew

28 www.theverge.com/22998479/lapsus-hacking-group-cyberattacks-news-updates

29 www.cnbc.com/2022/03/16/what-has-anonymous-done-to-russia-here-are-the-results-.htmlhttps://www.cnbc.com/2022/03/16/what-has-anonimo-renuncie-a-rusia-aqui-estan-los-resultados-.html

Entre las amenazas más comunes contra las infraestructuras críticas y los servicios esenciales figuran[30].

**Ataques de denegación de servicio y de denegación de servicio distribuida**

Las amenazas cibernéticas a las infraestructuras críticas a menudo incluyen intentos de interrumpir los servicios a través de ataques de denegación de servicio (DoS), que están diseñados para inundar un servidor con tráfico, haciendo que el sitio web o los servidores en línea de la infraestructura crítica no estén disponibles[31]. Además, un ataque DoS puede llevarse a cabo mediante el uso de múltiples ordenadores para inundar un sistema objetivo, conocido como un ataque de denegación de servicio distribuido (DDoS)[32]. El objetivo puede ser abrumar las redes de comunicación, haciéndolas incapaces de coordinarse y responder con eficacia[33].

**Explotación selectiva o interrupción de los sistemas de control industrial**

Las amenazas cibernéticas a las infraestructuras críticas a menudo implican la explotación selectiva o la interrupción de los sistemas de control industrial (ICS) y los sistemas de control de supervisión y adquisición de datos (SCADA), utilizados para gestionar y automatizar procesos críticos en sectores como la energía, el agua y la fabricación. A diferencia de los ciberataques típicos, que se centran principalmente en el robo de datos o la interrupción del sistema, los ataques contra infraestructuras críticas pueden tener como objetivo manipular procesos físicos. Por ejemplo, un ciberataque contra una red eléctrica podría intentar interrumpir el flujo de electricidad.

***Malware* sofisticado**

Las ciberamenazas a las infraestructuras críticas a menudo implican *malware* sofisticado y amenazas persistentes avanzadas. Estas amenazas están diseñadas para pasar desapercibidas durante largos periodos de tiempo, lo que permite a los atacantes recopilar información, escalar privilegios y llevar a cabo ataques coordinados con un impacto significativo[34].

**Explotación de vulnerabilidades de día cero**

Las vulnerabilidades de día cero son comúnmente recogidas y explotadas por los diversos tipos de ciberactores maliciosos. Estas vulnerabilidades son especialmente graves porque no hay forma de saber que están siendo explotadas hasta que se produce algún impacto real. El mercado clandestino de estas vulnerabilidades ofrece importantes beneficios ilícitos a quienes las descubren, que superan con creces las recompensas de los programas legales de recompensas por fallos de los proveedores de las tecnologías afectadas.

**Ingeniería social**

La ingeniería social se refiere a las tácticas utilizadas para explotar un comportamiento o error humano con el fin de obtener acceso a sistemas internos. Una de las tácticas más utilizadas es el *phishing*, en el que los atacantes adoptan una identidad falsa para enviar correos electrónicos o mensajes de texto o realizar llamadas a víctimas desprevenidas. El objetivo es engañarlas para que faciliten información crucial, como números de cuentas bancarias o contraseñas, o descarguen *malware* sin saberlo[35].

30 www.ericsson.com/en/blog/2023/10/deciphering-the-evolving-threat-landscape-security-in-a-5g-world

31 www.fortinet.com/resources/cyberglossary/dos-vs-ddos#:~:text=A%20denial%2Dof%2Dservice%20(,to%20flood%20a%20targeted%20resource.https://www.fortinet.com/resources/cyberglossary/dos-vs-ddos#:~:text=A%20denial%2Dof%2Dservice%20(,to%20flood%20a%20targeted%20resource

32 Ibid.

33 La escala de los ataques DDoS ha aumentado con el tiempo. Según las conclusiones de Google, un ataque DDoS masivo que bloquearon fue 7,5 veces mayor que el mayor ataque que habían bloqueado anteriormente en 2022. Emil Kiner & Tim April, Google mitigó el mayor ataque DDoS hasta la fecha, con un pico superior a 398 millones de rps www.cloud.google.com/blog/products/identity-security/google-cloud-mitigated-largest-ddos-attack- peaking-above-398-million-rpshttps://cloud.google.com/blog/products/identity-security/google-cloud-mitigated-largest-ddos-attack- peaking-above-398-million-rps

34 www.securelist.com/apt-trends-report-q3-2023/110752

35 www.cmu.edu/iso/aware/dont-take-the-bait/social-engineering.html

**Acceso físico y ataques híbridos**

Las infraestructuras críticas suelen implicar activos físicos como centrales eléctricas, presas y sistemas de transporte. Los actores de las amenazas pueden intentar acceder físicamente a estas instalaciones, ya sea directamente o a través de amenazas internas, para comprometer los sistemas desde dentro. Pueden emplear ataques híbridos, combinando diversas técnicas cibernéticas con acciones físicas. Las campañas multivectoriales pueden incluir componentes cibernéticos junto con otras formas de sabotaje o interrupción.

**Extorsión triple**

La triple extorsión es una táctica utilizada por los atacantes de *ransomware*, en la que, además de robar datos confidenciales de las organizaciones y amenazar con hacerlos públicos a menos que se efectúe un pago, también se dirigen a los clientes y/o socios comerciales de las organizaciones y les exigen rescates. Esto significa que los atacantes no sólo cifran los datos de la víctima y exigen un rescate por su liberación, sino que también exfiltran los datos y amenazan con hacerlos públicos y lanzar un ataque de denegación de servicio para presionar aún más a la víctima para que pague el rescate.

**Ataques a la cadena de suministro**

Atacar infraestructuras críticas a través de la cadena de suministro de software es uno de los posibles vectores de amenaza que pueden explotar los atacantes. Los ataques a la cadena de suministro son una forma creciente y cada vez más sofisticada de ciberamenaza. Su objetivo es la compleja red de relaciones entre las organizaciones clientes y sus proveedores, vendedores y terceros proveedores de servicios vitales para la cadena de suministro[36].

La Agencia Europea de Ciberseguridad (ENISA) ha propuesto una taxonomía de los ataques a la cadena de suministro, véase la **Figura 1**, que consta de cuatro partes:

i. técnicas de ataque utilizadas contra el proveedor,

ii. activos atacados en el proveedor,

iii. técnicas de ataque utilizadas contra el cliente,

iv. activos atacados en el cliente.

Un ataque a la cadena de suministro es una combinación de al menos dos ataques: el primero a un proveedor que luego se utiliza para atacar al objetivo y obtener acceso a sus activos. El objetivo puede ser el cliente final u otro proveedor. Por lo tanto, para que un ataque se clasifique como ataque a la cadena de suministro, tanto el proveedor como el cliente deben ser objetivos[37].

36 www.crowdstrike.com/cybersecurity-101/cyberattacks/supply-chain-attacks/https://www.crowdstrike.com/cybersecurity-101/cyberattacks/supply-chain-attacks/

37 En el ataque a la cadena de suministro de MOVEit, los atacantes, CI0p, aprovecharon una vulnerabilidad de la herramienta MOVEit Transfer para acceder a los datos almacenados en la base de datos. El incidente afectó a más de 620 organizaciones. www.cyberint.com/blog/research/recent-supply-chain- attacks-examined/https://cyberint.com/blog/research/recent-supply-chain-attacks-examined/

**Figura 1: Taxonomía de los ataques a la cadena de suministro**

| Proveedor | | Cliente | |
|---|---|---|---|
| **Técnicas de ataque utilizadas para comprometer la cadena de suministro** | **Activos de los proveedores objeto del ataque a la cadena de suministro** | **Técnicas de ataque utilizadas para comprometer al cliente** | **Activos de los clientes objeto del ataque a la cadena de suministro** |
| Infección por *malware* | Software preexistente | Relación de confianza | Datos |
| Ingeniería social | Bibliotecas informáticas | [T1199] | Datos personales |
| Ataque de fuerza bruta | Código | Compromiso Drive-by [T1189] | Propiedad intelectual |
| Aprovechamiento de la vulnerabilidad del software | Configuraciones<br>Datos | *Phishing* [T1566] | Software |
| Aprovechamiento de la vulnerabilidad de la configuración | Procesos | Infección por *malware* | Procesos |
| Inteligencia de fuentes abiertas (OSINT) | Hardware<br>Personas<br>Proveedor | Ataque físico o modificación | Ancho de banda<br>Finanzas |
| | | Falsificación | Personas |

Fuente: ENISA, Panorama de las amenazas a la cadena de suministro, 2021

## 2.3 Mayor complejidad en la respuesta a las amenazas contra las infraestructuras críticas

Además de la vasta red de agentes maliciosos y amenazas, una de las complejidades fundamentales para salvaguardar estos sistemas vitales reside en la sutil interacción entre los sectores público y privado, donde las responsabilidades en materia de ciberseguridad están a menudo entrelazadas.

### Colaboración público-privada y responsabilidades

Tanto si las infraestructuras críticas son gestionadas por el sector público como por el privado, o por una combinación de ambos, bajo la supervisión de las autoridades gubernamentales, es imperativo establecer una clara delimitación de deberes y obligaciones entre el sector privado y las autoridades gubernamentales para facilitar la ciberseguridad. En concreto, debería aclararse lo siguiente:

- **Funciones y responsabilidades verticales**: Las autoridades gubernamentales actúan como supervisoras, supervisando la dirección global y el objetivo general de los requisitos de ciberseguridad, así como las acciones de contingencia durante los incidentes cibernéticos. Por otro lado, las empresas son los profesionales, asumiendo las principales responsabilidades para mantener la rutina diaria de la ciberseguridad. La falta de una delimitación clara de las funciones y responsabilidades puede obstaculizar la eficacia de estas colaboraciones público-privadas. Por ejemplo, a pesar de la importancia de compartir la información, el sector privado podría mostrarse reacio a confiar a las autoridades su información corporativa sensible, ya que esto crea riesgos adicionales de filtraciones de datos no deseadas y posibles responsabilidades legales[38]. Dadas las complejidades de este caso, es crucial que todas las partes implicadas consideren colectivamente la opción de adoptar una solución alternativa..

38 www.gost.isi.edu/cctws/delroso-ghosh.PDFhttps://gost.isi.edu/cctws/delroso-ghosh.PDF

- **Funciones y responsabilidades horizontales:** Con mayor frecuencia, un ciberincidente puede implicar a múltiples autoridades gubernamentales, lo que complica las funciones y responsabilidades relativas a las infraestructuras críticas. Esto contribuye a menudo a las diferentes perspectivas sobre la delimitación de la autoridad entre la supervisión diaria y manejo de emergencias de ciberataque[39]. En vista de ello, es aconsejable que la delimitación de funciones y responsabilidades entre la autoridad central de supervisión, la autoridad local de supervisión y la autoridad de la ciberseguridad se definan cuidadosamente en una variedad de escenarios, que incluyen, entre otros, el mantenimiento diario, los incidentes cibernéticos y las auditorías posteriores a los incidentes. Además, el gobierno debe asegurarse de que tanto las autoridades como las entidades privadas implicadas entienden claramente estas delimitaciones.

**Implicaciones transfronterizas**

Algunas infraestructuras críticas, como las redes financieras o los cables submarinos, cruzan a menudo las fronteras nacionales, y las cadenas de suministro de infraestructuras críticas presentan incluso un mayor grado de vínculos internacionales. Además, las propias ciberamenazas no conocen fronteras. Todo esto crea complicaciones para las empresas que operan en varias jurisdicciones. Dado que las operaciones de las infraestructuras críticas pueden extenderse más allá de las fronteras nacionales, es importante reconocer que la ciberseguridad de las infraestructuras críticas y de las cadenas de suministro también estará sujeta a la influencia de los conflictos políticos mundiales, lo que repercutirá en la continuidad de las actividades de las infraestructuras críticas y de sus cadenas de suministro.

Por ejemplo, en el panorama mundial actual, algunos países están imponiendo restricciones a la importación y exportación de determinados bienes y tecnologías para salvaguardar su seguridad nacional. En consecuencia, las empresas que operan en múltiples jurisdicciones se enfrentan a crecientes retos de cumplimiento y a un aumento de los costes. Esta tendencia es especialmente evidente en el ámbito de la ciberseguridad, donde los gobiernos están tomando medidas para proteger sus infraestructuras críticas de posibles riesgos[40].

Además del conflicto geopolítico que conduce a restricciones en los componentes críticos, obstruyendo así el abastecimiento de componentes para la infraestructura crítica, la formulación dispar de políticas públicas sigue siendo el problema más amplio y profundo que nos ocupa. Como ya se ha dicho, aunque el principio general para identificar una infraestructura crítica es similar en todo el mundo, no existe una definición unificada de infraestructura crítica. Además, la incoherencia de las medidas de contingencia, los requisitos de información y los procesos de mejora tras los sucesos en los distintos países complican aún más el cumplimiento de la normativa por parte de las empresas que prestan servicios de infraestructuras críticas nacionales y transfronterizas y de los proveedores de las cadenas de suministro de infraestructuras críticas.

Por ejemplo, en algunas jurisdicciones, las autoridades competentes han designado a determinados proveedores de infraestructuras críticas para someterlos a una normativa más estricta. Estas regulaciones incluyen el establecimiento de planes integrales de mantenimiento de la ciberseguridad y la notificación obligatoria de cualquier incidente cibernético a las autoridades pertinentes tan pronto como tengan conocimiento de tales incidentes[41]. Por el contrario, otras jurisdicciones, como Japón, no identifican explícitamente a los proveedores de infraestructuras críticas. En su lugar, desarrollan sus políticas de ciberseguridad como directrices no vinculantes, por lo que no imponen una obligación a los proveedores de infraestructuras críticas de notificación de incidentes de ciberseguridad, a menos que dichos incidentes se refieran a violaciones de datos personales u otras industrias fuertemente reguladas. No obstante, tras la

39 En el caso de una empresa de oleoductos, las autoridades competentes responsables de supervisar la rutina diaria de la empresa deberían ser los sectores gubernamentales encargados de la energía y el transporte. Sin embargo, cuando se trata de hacer frente a un ciberataque, las autoridades competentes pueden ser los sectores responsables de la infraestructura de la información. Sin embargo, en el caso de un incidente cibercriminal, la empresa de oleoductos podría notificar únicamente a los sectores de la energía y el transporte los impedimentos de sus operaciones diarias, haciendo caso omiso del sector de la infraestructura de la información, que poseen capacidades más competentes para ofrecer sugerencias y prevenir la expansión de los daños. www.cybersolarium.org/csc-2-0-reports/revising-public-private-collaboration-to-protect-u-s-critical-infrastructure/https:// cybersolarium.org/csc-2-0-reports/revising-public-private-collaboration-to-protect-u-s-critical-infrastructure/

40 Tanto Estados Unidos como China han aplicado restricciones al uso de dispositivos y componentes específicos fabricados por el otro dentro de sus respectivas jurisdicciones con el fin de mitigar los riesgos potenciales. Con la creciente atención prestada a la ciberseguridad, este enfoque es cada vez más común, lo que se traduce en mayores costes de cumplimiento para las infraestructuras críticas que operan en múltiples jurisdicciones. www.time.com/6295902/china-tech-war-u-s/

41 www.ec.europa.eu/commission/presscorner/detail/el/MEMO_16_2422)

promulgación de la Ley de Promoción de la Seguridad Nacional a través de Medidas Económicas Integradas, las autoridades competentes de Japón iniciarán la identificación de los proveedores de infraestructuras críticas y emprenderán medidas adicionales de supervisión y regulación[42]. En resumen, se recomienda un marco estandarizado para la definición y aplicación de medidas para el funcionamiento de las infraestructuras críticas y la cooperación internacional.

**Implicaciones económicas**

Dado que las infraestructuras críticas prestan los servicios más fundamentales para la vida de las personas, las empresas a menudo tienen que hacer equilibrios entre ofrecer esos servicios vitales a un precio competitivo para los consumidores y garantizar que las infraestructuras críticas sean lo más resilientes posible. Los gobiernos deben ser conscientes de este hecho y pensar en cómo ayudar a las empresas a mejorar su resiliencia.

Como ya se ha mencionado, las infraestructuras críticas son vitales para el funcionamiento de un país y suelen ser construidas, explotadas y propiedad del sector privado. Para salvaguardar el bienestar básico del público, muchos gobiernos aplican regulaciones de precios a los servicios que son esenciales para el público, incluidos el agua, la energía y las telecomunicaciones, a menudo teniendo en cuenta la situación económica nacional. En consecuencia, la imposición de la regulación de precios puede obstaculizar la capacidad del sector privado para generar beneficios.

Por ejemplo, en Finlandia, la Ley del Mercado de la Electricidad es la legislación que rige el sector energético. Un aspecto crucial que aborda es el establecimiento de límites de tiempo de interrupción, acompañados de las correspondientes sanciones en forma de compensaciones a los consumidores. En la enmienda de 2013, la Ley del Mercado de la Electricidad introdujo requisitos adicionales para que los operadores cumplan los objetivos de resiliencia frente a los riesgos meteorológicos, que deberán cumplir antes de finales de 2028 y están obligados a presentar un plan de inversiones a la autoridad energética cada dos años para demostrar sus progresos. Por otro lado, la normativa permitía a estos operadores subir los precios de distribución, hasta un incremento máximo del 30% en algunos casos. Sin embargo, debido a la fuerte reacción pública y política, el aumento de precios se limitó posteriormente al 15% anual, lo que creó problemas de liquidez a algunos operadores. Este ejemplo pone de relieve que, a pesar de la importancia de mejorar la resiliencia de las infraestructuras críticas, es igualmente importante equilibrar las expectativas públicas y los incentivos y precios de los operadores[43].

Dado el carácter lucrativo del sector privado, es aconsejable que las autoridades gubernamentales promuevan la ciberseguridad entre los proveedores de infraestructuras críticas mediante la aplicación de deducciones fiscales, préstamos con tipos de interés preferenciales, subvenciones y otros incentivos.

42 www.iclg.com/practice-areas/cybersecurity-laws-and-regulations/japanhttps://iclg.com/practice-areas/cybersecurity-laws-and-normativa/japón

43 https://www.oecd-ilibrary.org/sites/02f0e5a0-en/1/2/4/index.html?itemId=/content/publication/02f0e5a0-en&_csp_=eb11192b2c569d5c3d1424677826106a&itemIGO=oecd&itemContentType=book

# 3. Protección de infraestructuras críticas y cadenas de suministro: ¿dónde estamos ahora?

## 3.1 Proteger las infraestructuras críticas y los servicios esenciales

Los mecanismos para aplicar la protección digital a infraestructuras críticas (digitales o no) y servicios esenciales son ya bien conocidos y, al margen de los nuevos riesgos que puedan surgir con la llegada de nuevos paradigmas como la IA o la computación cuántica, los procesos básicos de seguridad pueden identificarse en cualquiera de los marcos estándar de ciberseguridad que diversas organizaciones (ISO, NIST, ISF, etc.) han venido desarrollando en las últimas décadas. La verdadera dificultad proviene de la imposibilidad de protegerlo todo por una simple cuestión de eficiencia o incluso de eficacia (los ecosistemas complejos no pueden asegurarse con procesos simples, ya que requieren segmentación para una protección focalizada).

**Buenas prácticas del sector**

En respuesta a las amenazas cibernéticas, el sector privado refuerza la resiliencia y la recuperación mediante la adopción de medidas de seguridad integrales, incluido el mantenimiento de inventarios de activos sólidos, el desarrollo de planes de respuesta a incidentes, la implementación de copias de seguridad de datos robustas, la garantía de sistemas actualizados con los últimos parches de seguridad y arquitecturas de confianza cero, así como una política de cadena de suministro robusta. La formación en ciberseguridad también entra en juego como un componente crucial, proporcionando a los empleados los conocimientos necesarios sobre las mejores prácticas, con el objetivo de construir una sólida postura de seguridad de los sistemas y servicios desde dentro hacia fuera.

**En general, las empresas recomiendan las siguientes herramientas y buenas prácticas para prevenir o atajar los ataques a la ciberseguridad:**

- Mantener un inventario eficaz de activos y una sólida vigilancia del perímetro con herramientas de gestión de vulnerabilidades. Esto es especialmente importante para la protección de infraestructuras críticas.
- Hacer copias de seguridad periódicas de los datos importantes, almacenados en un sistema debidamente protegido.
- Establecer políticas de privilegios de seguridad para restringir el acceso de usuarios innecesarios, al tiempo que se mantienen los sistemas actualizados con los últimos parches de seguridad. Esto es especialmente relevante en el caso de los sistemas OT con acceso a infraestructuras no replicadas o críticas para la seguridad.
- Utilización de sistemas de detección y respuesta de puntos finales (EDR), incluida la autenticación multifactor para los activos expuestos públicamente.
- Implantación de soluciones avanzadas de detección y respuesta entre capas en todas las plataformas.
- Emplear firmas antivirus actualizadas y configurar cortafuegos a nivel de aplicación.
- Prestar atención a las vulnerabilidades de los dispositivos de copia de seguridad y almacenamiento, el software VPN y las puertas de enlace, y parchear el software para solucionar las vulnerabilidades de las aplicaciones de servidor y cliente.
- Aplicación de los principios de confianza cero en toda la arquitectura de red.

- Añadir capacidades de ciberdefensa (basadas en SOC - Security Operation Centre) a los procesos, tecnologías y operaciones, así como el desarrollo de planes detallados de respuesta a incidentes (IRP), con procedimientos para estrategias de respuesta a incidentes y proporcionar equipos dedicados de respuesta a incidentes (IRT).
- Ante las posibles interrupciones operativas y las cargas financieras, los proveedores de servicios esenciales recurren cada vez más a partenariados e iniciativas de cooperación como piedra angular de su protección. El seguimiento de las tendencias de los ciberataques, el intercambio de información y la colaboración con las autoridades regionales y otros proveedores de servicios esenciales son fundamentales.
- En los casos de ciberataques, desplegar una investigación forense para analizar todo el modus operandi empleado por los atacantes, evaluar las vulnerabilidades que realizaron el acceso inicial e identificar si el ciberdelincuente accedió a información sensible o vulneró la integridad permite mejoras futuras.
- Impartir formación sobre ciberseguridad para educar a los empleados, realizar auditorías de seguridad periódicas para probar los mecanismos y minimizar la exposición externa a las redes internas.
- Considerar que la cadena de suministro es clave no sólo para mantener la eficiencia y la calidad del servicio a los clientes, sino también para garantizar que el compromiso potencial de un elemento de la cadena no afecte a otros elementos y al servicio en su conjunto. Este ha sido el caso en algunos de los incidentes recientes más sonados (*SolarWinds*, Colonial, más recientemente las vulnerabilidades de Ivanti VPN, etc.).
- Considerar el soporte bajo demanda y la formación de equipos de defensa coordinados que operen a través de las fronteras nacionales para proporcionar respuestas rápidas y eficaces durante incidentes cibernéticos a gran escala. Estos equipos desempeñarán un papel fundamental a la hora de mitigar el impacto de ciberamenazas significativas en infraestructuras críticas[44].

So, which are the key aspects that should prevail in order to significantly improve the level of resiliency of essential services and critical infrastructure protection? To minimise the impact of potential disruptive situations, essential service providers need to build resilience and adopt best practices in risk management to protect critical infrastructures and end-to-end services.

**Adoptar la nueva forma de trabajar de Business Under Disruption implica trabajar en aspectos como:**

- Identificar los activos y servicios esenciales y definir los tiempos de inactividad y recuperación.
- Comprender la interconexión de la empresa con otras empresas, con especial atención a la cadena de suministro.
- Utilización de escenarios de riesgo vinculados, actualización del mapa de riesgos y escenarios de eventos concurrentes. Deben abarcar actividades como la identificación (de activos), la protección, la prevención, la detección, la respuesta, la recuperación, el aprendizaje, la evolución y la comunicación. La gestión de riesgos incluirá la estrategia de resiliencia operativa digital, incluidos, entre otros, los indicadores de rendimiento, el tratamiento de las desviaciones, los parámetros de medición de riesgos, la ejecución de pruebas, la notificación de incidentes, las auditorías, etc. para alcanzar los objetivos específicos de las TIC, así como, entre otros, la metodología de análisis de riesgos para la confidencialidad, integridad, disponibilidad y autenticidad de la información.
- Realización de pruebas en sistemas en producción y determinación del nivel de sensibilización.

44 www.digital-strategy.ec.europa.eu/en/policies/cyber-solidarity

**Enfoques de políticas públicas y normativos de la ciberseguridad de las infraestructuras críticas**

Como se ha dicho anteriormente, cualquiera de los marcos de ciberseguridad existentes es suficiente en sí mismo para aumentar la resiliencia de dichos servicios e infraestructuras (en el ámbito digital). Algunos ejemplos son el Marco de Ciberseguridad (CSF) del NIST o la recientemente actualizada ISO27001:2022, que incorpora el enfoque más estructurado del SGSI (sistema de gestión de la seguridad de la información).

Diferentes regímenes reguladores pretenden contribuir estableciendo requisitos (en lugar de normas), como el DORA para el sector financiero o el NIS2 para los proveedores digitales y la Ley de Resiliencia de la Ciberseguridad, que abarcan no sólo las infraestructuras críticas, sino también los productos digitales. Las mejores prácticas aún están por afianzarse una vez que el reglamento DORA esté en vigor y la Norma Técnica Reglamentaria (NTR) se publicará en 2024. Sin embargo, ya se puede empezar a trabajar en el cumplimiento de los requisitos de diseño para garantizar una base sólida para la resiliencia operativa digital de las empresas y entidades críticas.

Sin embargo, la dinámica de los mercados de los distintos servicios impone severas limitaciones a la hora de exigir y evaluar los requisitos de seguridad de un proveedor de servicios clave. Si bien las certificaciones de los marcos de ciberseguridad sirven a este propósito, siguen siendo limitadas en un escenario de márgenes empresariales decrecientes, en el que todas las partes de los servicios buscan reducir costes y eficiencias para recortar gastos en controles (controles de seguridad, en este caso).

Asimismo, a nivel nacional existen diferentes normativas para implementar marcos más genéricos y facilitar el control posterior del cumplimiento por parte de los organismos reguladores.

Por ejemplo, el ENS en España para el sector público, la TSA en el Reino Unido para los proveedores de servicios de comunicación. En China, el Ministerio de Transporte publicó las Medidas de Gestión de Protección de la Seguridad de las ICI para el sector del transporte, que requiere que los operadores de ICI en el sector del transporte cumplan con una serie de obligaciones de cumplimiento. En Australia, la Ley de Seguridad de las Infraestructuras Críticas (SOCI) (2018)[45] define las infraestructuras críticas como "infraestructuras críticas" y establece sus obligaciones. En el marco de una importante estrategia nacional de ciberseguridad de amplio alcance (2023-2030)[46], el Gobierno está elaborando una serie de modificaciones clave de la SOCI que, entre otras cosas, incluirá los sistemas de almacenamiento de datos en el ámbito de los datos críticos para las empresas (de un activo de infraestructura crítica), mejorará las respuestas nacionales a incidentes significativos, simplificará la gestión de los datos por parte del Gobierno y aumentará la seguridad de los datos, el intercambio de información del sector en situaciones de crisis, y la consolidación de los requisitos de seguridad de las telecomunicaciones en una sola ley. Estas modificaciones (y la estrategia en general) pretenden garantizar la protección de las entidades y activos adecuados, asegurar el cumplimiento de las obligaciones de ciberseguridad y proporcionar la ayuda necesaria a las infraestructuras críticas para gestionar las consecuencias de los incidentes cibernéticos.

Es necesario establecer una correspondencia adecuada entre estos marcos, ya que en muchos casos los proveedores de servicios esenciales tienen que hacer frente a diferentes exigencias normativas en función de la geografía y los sectores de actividad (por ejemplo, una rama financiera de un proveedor de servicios de Internet puede tener que cumplir tanto la normativa de telecomunicaciones como la financiera, y otra serie de normas en función de los países y los clientes a los que preste sus servicios).

45 www.legislation.gov.au/C2018A00029/latest/text
46 www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf

## 3.2 Asegurar la cadena de suministro de infraestructuras críticas

El estado actual de la gestión del riesgo en la cadena de suministro cibernética (C-SCRM) en los sectores de infraestructuras críticas a nivel mundial es difícil de generalizar. Por un lado, es justo decir que una parte significativa de la infraestructura crítica en algunos mercados es propiedad y está operada por el sector privado. En Estados Unidos, las estimaciones oficiales sitúan la propiedad privada de las infraestructuras críticas en el 85%[47]. En la UE, es del 80%[48]. En el Reino Unido, aproximadamente el 50% de las infraestructuras críticas son de propiedad y gestión privada[49], mientras que en muchos otros mercados, como China, Oriente Medio y otros, la propiedad estatal de las infraestructuras críticas es el modelo predominante.

Por otro lado, sin embargo, las diversas entidades del sector privado y estatal que constituyen la comunidad mundial de propietarios y operadores de infraestructuras críticas son tan diversas como numerosas. Estas entidades abarcan desde grandes corporaciones multinacionales hasta pequeños productores independientes, proveedores de servicios, contratistas independientes y subcontratistas.

Aparte de la diferencia en los modelos de propiedad entre países, la definición y, por tanto, el alcance de lo que se considera una infraestructura crítica en una jurisdicción determinada varía de un país a otro, desde ninguna a definiciones y marcos exhaustivos, como se muestra en el anexo I. Las diferencias en las definiciones clave, entre otras, pueden dar lugar a problemas de política internacional, cuando se trata de desarrollar las mejores prácticas y normas internacionales destinadas a reforzar la ciberseguridad y la resiliencia de las infraestructuras críticas a nivel regional o mundial.

El Global Cybersecurity Outlook 2024 del Foro Económico Mundial[50] identificó, entre otras cosas, una creciente brecha de ciberresiliencia entre las grandes, pequeñas y medianas empresas, lo que pone de relieve un desafío adicional cuando se considera la seguridad y la resiliencia de las cadenas de suministro de infraestructuras críticas.

La situación se agrava aún más por la ampliación de la superficie de amenaza, al conectarse a través de tecnologías operativas IoT que controlan los sistemas de energía, agua, alcantarillado y otras infraestructuras críticas. Dado que la práctica del "*air gapping*", o segregación física de las redes digitales, ha dado paso a las exigencias de una interconectividad más amplia a través de la tecnología IoT y la integración de sistemas heredados con software más moderno, las brechas en la cadena de suministro se han convertido en un vector de ataque favorecido por los actores maliciosos.

De ello se desprende, por tanto, que todas estas entidades que operan en infraestructuras críticas tienen distintos modos de propiedad, se enfrentan a diferentes marcos normativos y poseen diferentes grados de recursos, experiencia y capacidad para asegurar adecuadamente las operaciones y sus cadenas de suministro.

**¿En qué consiste la ciberseguridad de la cadena de suministro?**

Como en la seguridad en general, la ciberseguridad es también una actividad de gestión de riesgos, ya que no existe la seguridad al 100%. En principio, los procedimientos de gestión de riesgos constan de cuatro tareas fundamentales: identificación de riesgos, evaluación y medición de riesgos, tratamiento y supervisión. El Gobierno australiano ofrece un ejemplo descriptivo de alto nivel de un proceso de gestión de riesgos[51].

Explotar las vulnerabilidades de las cadenas de suministro de software existentes en lugar de dirigirse a los usuarios finales ha permitido a estos actores ampliar su impacto comprometiendo varias empresas simultáneamente y penetrando subrepticiamente en cuentas en las que puede ser más difícil infiltrarse directamente.

Aunque las infiltraciones cibernéticas en la cadena de suministro no son un fenómeno completamente nuevo, con múltiples violaciones conocidas de la cadena de suministro que se remontan a 2013[52], el descubrimiento de la violación de la plataforma de monitorización y gestión de IT Orion de Solar Winds en diciembre de 2021

47 www.gao.gov/products/gao-09-654r
48 www.gisreportsonline.com/r/europe-critical-infrastructure/
49 www.nic.org.uk/temas/diseño-financiación/
50 www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf
51 www.austrac.gov.au/business/core-guidance/amlctf-programs/implement-risk-management-process
52 www.reversinglabs.com/blog/a-partial-history-of-software-supply-chain-attacks

marca un hito en el crecimiento de este vector de amenaza. Statista, la plataforma en línea de estadísticas y encuestas, informa de que el número de paquetes de software afectados en todo el mundo en ataques conocidos a la cadena de suministro aumentó de 700 en 2019 a más de 185.000 en 2022[53] y no termina. Gartner predice que, para 2025, el 45 % de las organizaciones de todo el mundo habrán sufrido ataques a sus cadenas de suministro de software, tres veces más que en 2021[54]. Se espera que las pérdidas económicas totales por ataques a la cadena de suministro, aunque sean una fracción del coste agregado de los ciberataques[55] crezcan exponencialmente. Cybersecurity Ventures, uno de los principales investigadores en ciberseguridad, prevé que las pérdidas económicas para las empresas mundiales derivadas de los ataques a la cadena de suministro crecerán un 15% interanual durante los próximos años. Así, se espera que el coste estimado para 2023 de 45.000 millones de dólares aumente hasta los 138.000 millones de dólares en 2031.

La buena noticia es que los gobiernos y la industria han empezado ser conscientes de ello y están tomando medidas. Existe un reconocimiento generalizado de que, para lograr una seguridad más eficaz de la cadena de suministro, los profesionales deben abordar el problema de forma integral. Por ejemplo, para mitigar el riesgo de la cadena de suministro de software es necesario incorporar prácticas de seguridad sólidas en el proceso de codificación interna al principio del ciclo de desarrollo del producto, asegurando el software comercial de terceras partes, así como el software de código abierto. Así, en organizaciones bien dotadas de recursos con programas de seguridad maduros, los desarrolladores han adoptado prácticas como revisiones coherentes del código, una disciplinada gestión interna de las vulnerabilidades y exigentes protocolos de aplicación de parches, especialmente en lo que se refiere a las dependencias de terceros[56].

**Buenas prácticas del sector**

En cuanto a la protección de la cadena de suministro, podría considerarse el uso de mejores prácticas[57] como las que se indican a continuación[58]:

1. **Centrarse en un conjunto de requisitos de seguridad prioritarios** basados en una evaluación del riesgo, una lista corta en lugar de sobrecargar al proveedor, y garantizar el seguimiento, la supervisión y el cumplimiento. Además, tener en cuenta las referencias y recomendaciones del sector cuando estén disponibles, como la IEC 62443 en ciberseguridad industrial.

2. **Reducir el impacto de los incidentes de terceros mediante acciones discretas** como diversificar la cadena de suministro, aplicar políticas de confianza cero[59], elaborar planes de respuesta a incidentes, realizar pruebas y exigir a los proveedores la notificación temprana de los incidentes.

3. **Asociarse activamente con los proveedores** para ayudarles a mejorar sus programas de seguridad, ofreciéndoles mecanismos de servicio y formación para protegerse de los incidentes o responder a ellos cuando se produzcan. Los incidentes de terceros ocurrirán, por lo que prepararse para gestionar el impacto en la empresa debe ser una prioridad fundamental.

4. **Considerar la posibilidad de aprovechar tecnologías emergentes** como *blockchain* para el intercambio de información y la gestión de activos con el fin de minimizar las consecuencias de los incidentes cibernéticos de terceros, así como la inteligencia artificial y la analítica avanzada para ampliar las capacidades de detección y respuesta ante incidentes.

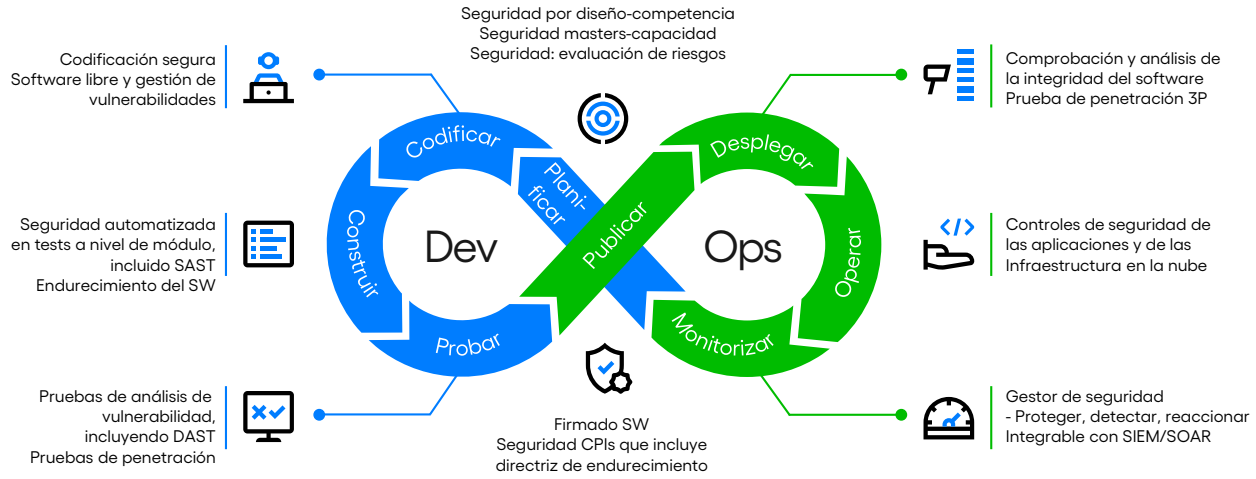
5. **Añadir incentivos y medidas coercitivas a los contratos**, estableciendo requisitos para los proveedores basados en normas internacionales (por ejemplo, ISO 27001 Seguridad de la información, ISO 27701 Privacidad, ISO 22301 Seguridad y resiliencia).

6. **Establecer procesos para aumentar la implicación de los líderes empresariales** en la gestión de los ciberriesgos de terceros. Hacerlo debe ser una prioridad en los niveles más altos.

53 www.statista.com/statistics/1375128/supply-chain-attacks-software-packages-affected-global/
54 www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-security-and-risk-management-trends-for-2022
55 www.weforum.org/publications/global-cybersecurity-outlook-2024/
56 www.go.snyk.io/2023-supply-chain-attacks-report-dwn-typ.html?aliId=eyJpIjoidFd0SVpwb0R6M2VNeUMrMyIsInQiOiJGRUE3VFdwTDB4Tk95TzkzTERadzRPT0ifQ%253D%253D
57 www.cybertechaccord.org/best-practice-alignment-for-supply-chain-security-across-standards-and-regulatory-frameworks/
58 www.email.rsaconference.com/p/7K6E-7LN/nur-48-2023esaf-formhttps://email.rsaconference.com/p/7K6E-7LN/nur-48-2023esaf-form
59 www.cybertechaccord.org/zero-trust-once-again/

En el contexto de la gestión de riesgos de la cadena de suministro de las TIC, por ejemplo, un proceso de gestión de riesgos de la cadena de suministro[60] podría abarcar el desarrollo interno de software, el consumo de software de terceros, incluido el software de código abierto, las prácticas de codificación segura, el escaneado de vulnerabilidades, las pruebas de vulnerabilidad y las pruebas de penetración, y operaciones. Es importante reconocer que la seguridad de la cadena de suministro de software es sólo un elemento de la seguridad de la cadena de suministro, pero desde la perspectiva de la ciberseguridad, es un elemento clave a tener en cuenta. Debido a la evolución tecnológica en la forma en que se desarrolla y entrega el software, como la integración continua y la entrega continua (CI/CD) flujo de trabajo, DevSecOps[61] ha evolucionado para abordar la necesidad de incorporar la seguridad de forma continua en todo el ciclo de vida de desarrollo del software. Otro avance importante en el mundo de las aplicaciones es la interfaz de programación de aplicaciones (API). En pocas palabras, una API es un tipo de software que actúa como interfaz o punto de conexión, permitiendo que dos aplicaciones o funciones diferentes se comuniquen entre sí. Desde los bancos, el comercio minorista y el transporte, hasta las redes de comunicación, el IoT, los vehículos autónomos y las ciudades inteligentes, las API son una parte fundamental de las aplicaciones móviles, del software como servicio (SaaS) y webs modernas, y pueden encontrarse en aplicaciones orientadas al cliente, a los socios o internas. Tomando estos y otros avances tecnológicos, en la **figura 2** se visualiza una cadena de suministro de software segura basada en SRM.

## Figura 2: Seguridad de la cadena de suministro de software basada en el modelo de fiabilidad de la seguridad de Ericsson




*Fuente: Ericsson, Modelo de Fiabilidad de la Seguridad, 2021*

### Seguridad del software de código abierto

Muchos proveedores de TIC y de servicios de comunicaciones aprovechan el software de código abierto (OSS) para sus proyectos y productos de software con el fin de permitir a los proveedores de servicios de comunicaciones construir redes abiertas e interoperables a menor coste. Ejemplos de colaboraciones industriales que promueven el uso de código abierto son la Open Network Automation Platform (ONAP) y la O-RAN Software Community (OSC), auspiciadas por la Linux Foundation, y Openstack, auspiciada por la OpenInfra Foundation. El OSS tiene beneficios inherentes que pueden proporcionar código seguro, pero también tiene riesgos de seguridad inherentes que requieren un mayor nivel de diligencia debida. Es la responsabilidad del proveedor del producto de software garantizar que existen las salvaguardas adecuadas para el uso seguro del producto enviado con componentes de OSS y software propietario.

La Open Source Security Foundation (OpenSSF) es otra organización que promueve normas para garantizar el código abierto en todo el sector[62].

60 www.ericsson.com/en/security/ericssons-security-reliability-model
61 www.synopsys.com/glossary/what-is-devsecops.html
62 www.openssf.org/

El uso de software de código abierto requiere un mayor nivel de diligencia debida que las organizaciones pueden poner en práctica aplicando las mejores prácticas de la industria para la gestión de la cadena de suministro, el desarrollo seguro de software y el mantenimiento seguro de software. Existen organizaciones gubernamentales e industriales que pueden ayudar, como DARPA AIxCC[63], el Instituto Nacional de Normalización (NIST) del Departamento de Comercio de EE.UU., la Fundación Linux, y OWASP. La Linux Foundation Core Infrastructure Initiative cuenta con un distintivo de buenas prácticas para proyectos de código abierto. La OWASP ha puesto a disposición de los proyectos de código abierto numerosas herramientas de detección automática de vulnerabilidades.

Según CISA[64] para asegurar el software de código abierto, es importante comprender los ataques y vulnerabilidades relevantes. A CISA le **preocupan en general dos clases distintas de vulnerabilidades y ataques al software de código abierto**:

1. Los efectos en cascada de las vulnerabilidades en el software de código abierto ampliamente utilizado. Como demuestra la vulnerabilidad *Log4Shell*, la ubicuidad del software de código abierto puede hacer que las vulnerabilidades tengan consecuencias especialmente generalizadas. Dada la prevalencia del software de código abierto en gobierno y las infraestructuras críticas, incluido el amplio uso de software de código abierto en software de código cerrado, la naturaleza generalizada y distribuida del software de código abierto puede magnificar el impacto de las vulnerabilidades del software de código abierto.

2. Ataques a la cadena de suministro de repositorios de código abierto que comprometen el software derivado. La segunda categoría de riesgos es el compromiso malintencionado de componentes de software de código abierto, que conduce a compromisos posteriores. Los ejemplos incluyen a un atacante que compromete la cuenta de un desarrollador e introduce código malicioso, o a un desarrollador que inserta intencionadamente una puerta trasera en su paquete. Algunos ejemplos reales son la incrustación de mineros de criptomonedas en paquetes de código abierto, la modificación del código fuente con software de protesta que borra los archivos de un usuario y el empleo de ataques de *typosquatting* que se aprovechan de los errores de los desarrolladores.

**Enfoques de políticas públicas y normativos de la ciberseguridad de las cadenas de suministro**

La globalización de la cadena de suministro de las empresas plantea nuevos retos para garantizar una gestión eficaz de los riesgos en consonancia con los intereses de la seguridad nacional, lo que puede exigir requisitos a medida.

De hecho, los gobiernos de todo el mundo están utilizando el poder de la regulación y la legislación para fomentar y, en algunos casos, imponer prácticas seguras de desarrollo de software. En EE.UU., la Administración Biden emitió la Orden Ejecutiva sobre la Mejora de la Ciberseguridad de la Nación (OE 14028) en mayo de 2021, tras el descubrimiento de la brecha de *SolarWinds*. Entre otras cosas, la OE ordenaba que el software comercial utilizado por el gobierno federal debía cumplir ciertas directrices. Estas directrices, desarrolladas por el Instituto Nacional de Estándares y Tecnología (NIST) y publicadas en dos documentos separados en febrero de 2022, la Publicación Especial (SP) 800-218 del NIST: Recommendations for Mitigating the Risk of Software Vulnerabilities (Recomendaciones para mitigar el riesgo de vulnerabilidades del software) y la NIST Software Supply Chain Security Guidance (Guía de seguridad de la cadena de suministro de software del NIST) exigen a las agencias federales y a los proveedores del sector privado que contratan con el gobierno federal que empleen medidas como el cifrado, la supervisión continua, autenticación multifactor, gestión de vulnerabilidades, listas de materiales de software (SBOM) y muchos otros requisitos. Aunque todavía no son obligatorias para los proveedores del sector privado fuera del ámbito de la contratación pública, el uso de estas directrices establece un estándar de seguridad de la cadena de suministro ampliamente reconocido y fomentado, cuyos elementos pueden llegar a ser obligatorios en la legislación y/o reglamentación posteriores.

63 www.aicyberchallenge.com/

64 www.cisa.gov/sites/default/files/2024-02/CISA-Open-Source-Software-Security-Roadmap-508c.pdf

En septiembre de 2022, la Comisión Europea propuso la Ley de Ciberresiliencia (CRA) para mejorar la ciberseguridad y la ciberresiliencia en la UE. La CRA pretende establecer normas de seguridad comunes para todos los productos con elementos digitales en la UE. La CRA exigirá a los fabricantes de productos con elementos digitales que apliquen medidas de ciberseguridad adecuadas a lo largo del ciclo de vida del producto. Esto incluirá la conformidad con los "requisitos esenciales de ciberseguridad" durante la fase de diseño y desarrollo, con evaluaciones iniciales de ciberseguridad y una gestión y actualización continuas de las vulnerabilidades, así como la notificación de incidentes durante todo el ciclo de vida del producto. En diciembre de 2023 se alcanzó un acuerdo común sobre el texto final de la CRA y se espera la aprobación definitiva del Parlamento Europeo y la Comisión Europea en 2024. Además, el recientemente aprobado Reglamento (UE) 2022/2554 sobre la resiliencia operativa digital en el sector financiero (DORA), aplicable a partir de enero de 2025, pondrá a prueba la protección de la cadena de suministro. Incluye disposiciones sobre contratos, normas de seguridad, gestión de riesgos, derechos de acceso, inspección y auditoría de proveedores, formación y concienciación sobre riesgos y resiliencia para el personal y estructuras de gobernanza para la gestión de la seguridad, entre otras.

La GSMA y el NIST han elaborado directrices de seguridad de la IoT para los fabricantes y los terceros que les prestan apoyo en la concepción, el diseño, el desarrollo, las pruebas, la venta y la asistencia de dispositivos de IoT en toda su gama de clientes. Según la GSMA, para que el IoT siga evolucionando eficazmente, deben abordarse los siguientes retos de seguridad:

- **Disponibilidad**: garantizar una conectividad constante entre los puntos finales y sus respectivos servicios.
- **Identidad**: autenticación de puntos finales, servicios y el cliente o usuario final que opera el punto final.
- **Protección de la intimidad**: reducir los posibles perjuicios a los usuarios finales
- **Seguridad**: garantizar que la integridad del sistema pueda verificarse, rastrearse y controlarse.

Las medidas de mitigación de la seguridad del IoT deben adaptarse a los clientes, las aplicaciones o los entornos. La adaptación puede ser para sectores empresariales o industrias verticales y puede añadir requisitos, editar requisitos específicos reduciendo o ampliando la forma en que se aplican o, en raras ocasiones, eliminar requisitos.

En octubre de 2022, el Centro Nacional de Ciberseguridad del Reino Unido (NCSC) publicó una guía para que las medianas y grandes organizaciones "se aseguren de la ciberseguridad de la cadena de suministro de su organización"[65]. La guía describe cómo las organizaciones están expuestas a vulnerabilidades y ciberataques a través de su cadena de suministro y define los resultados esperados y los pasos clave para ayudar a las organizaciones a evaluar la seguridad de su cadena de suministro. Las directrices son voluntarias y actualmente no existe en el Reino Unido una legislación obligatoria en materia de seguridad de la cadena de suministro. En la actualidad, el Reino Unido está tratando de encontrar un vehículo legislativo adecuado para actualizar las directrices de la UE en materia de seguridad de la Directiva sobre Sistemas de Redes e Infraestructuras (NIS) de 2018, que espera cumplir en 2024. Las enmiendas propuestas incluyen muchas de las mismas medidas de seguridad de la cadena de suministro que se discuten en la legislación/regulación de EE.UU. y la UE. Además, la Ley de Seguridad de Productos e Infraestructura de Telecomunicaciones de 2022 (PSTIA) del Reino Unido, reproduce muchas de las disposiciones de la CRA con respecto a los productos digitales, incluida la transparencia sobre los períodos mínimos de soporte de seguridad y notificación de vulnerabilidades, así como la prohibición de contraseñas predeterminadas. Estas disposiciones entrarán en vigor en abril de 2024.

65 www.ncsc.gov.uk/collection/assess-supply-chain-cyber-security

En China, las Medidas de Revisión de la Ciberseguridad (CRM) publicadas por la Administración de Ciberseguridad de China (CAC) en diciembre de 2021, establecieron un mecanismo de revisión de la ciberseguridad para la contratación por parte de la CII de productos y servicios de red, que afectan o pueden afectar a la seguridad nacional. Además, el Ministerio de Industria y Tecnología de la Información (MIIT) y la CAC publicaron las Disposiciones Administrativas sobre Vulnerabilidades de Seguridad de Productos Cibernéticos. Estas disposiciones obligan a los proveedores de ciberproductos a tomar medidas para gestionar las vulnerabilidades de seguridad de los ciberproductos e informar de ellas a la Plataforma de Intercambio de Información sobre Amenazas y Vulnerabilidades de Ciberseguridad[66].

También hay iniciativas en marcha en otros mercados, como las orientaciones del Centro Canadiense de Ciberseguridad sobre la protección de las organizaciones frente a las amenazas a la cadena de suministro de software[67] o las del Centro Nacional de Ciberseguridad de Nueva Zelanda sobre la ciberseguridad de la cadena de suministro[68]. No obstante, aún queda mucho por hacer.

El objetivo debe ser lograr unos requisitos armonizados en todos los mercados, basados en las mejores prácticas empresariales y en normas internacionales. Muchos de los esfuerzos realizados en el pasado para armonizar los requisitos y las evaluaciones no han logrado alcanzar un acuerdo y, lamentablemente, han aumentado la complejidad del cumplimiento, incrementando así el riesgo. Como resultado, está resultando difícil y costoso para los contratistas principales de servicios específicos comprender y gestionar los riesgos de múltiples subcontratistas.

La cooperación internacional en materia de obligaciones de notificación de incidentes para los operadores de infraestructuras críticas es otro ámbito de cooperación bienvenido en el que la armonización internacional puede reducir la complejidad y las cargas administrativas y, al mismo tiempo, garantizar la disponibilidad de información pertinente y oportuna para aumentar el conocimiento de la situación y, con el tiempo, ampliar el conocimiento acumulado. Para avanzar en este sentido, las medidas adoptadas por los EE.UU. y la UE para racionalizar las obligaciones de notificación de incidentes deberían seguir fomentándose y, con el tiempo, ampliarse geográficamente en los foros internacionales pertinentes[69].

**Además, para mantener la resiliencia, seguridad, confianza y competitividad de las redes y cadenas de suministro, la diversificación es clave.** Las decisiones de seguridad nacional que restringen los componentes críticos o sensibles de proveedores específicos deben basarse en criterios objetivos, ser proporcionadas y aplicarse eficazmente. La exclusión de proveedores puede tener un alto impacto en los costes de los operadores privados de infraestructuras críticas, pero también en la seguridad nacional, la resiliencia y el desarrollo del mercado. Por lo tanto, estas decisiones también deben tener en cuenta que los operadores privados de infraestructuras críticas no son responsables de la seguridad nacional ni tienen necesariamente en cuenta los riesgos para la seguridad nacional en sus decisiones empresariales.

Un enfoque cooperativo y coordinado entre todas las partes interesadas es el mejor medio de que disponen los gobiernos para elevar las normas básicas de ciberseguridad, evitando el exceso de información y generando al mismo tiempo una práctica común eficiente basada en la confianza, especialmente en la cadena de suministro. Para reducir los ciberataques y aumentar así la seguridad, es esencial adoptar un enfoque holístico, reforzar la cooperación entre las distintas partes interesadas para luchar contra la ciberdelincuencia y aplicar normas de comportamiento estatal responsable en el ciberespacio.

66 www.reuters.com/technology/china-conduct-cybersecurity-review-chipmaker-microns-products-2023-03-31
67 www.cyber.gc.ca/en/guidance/protecting-your-organization-software-supply-chain-threats-itsm10071
68 www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Supply-Chain-Cyber-Security.pdf
69 https://digital-strategy.ec.europa.eu/en/library/comparative-assessment-dhs-harmonization-cyber-incident-reporting-federal-government-report-and

# 4. Hacia una mejor protección de las infraestructuras críticas y una mayor seguridad de la cadena de suministro

La protección de la ciberseguridad de los servicios esenciales y las infraestructuras críticas y sus cadenas de suministro requiere un enfoque equilibrado, bien orientado y proporcionado para todos los proveedores de servicios de infraestructuras críticas y servicios esenciales, junto con un marco regulador nacional e internacional adecuado con suficiente capacidad pública para hacer cumplir e incentivar un comportamiento adecuado.

**Dado que la ciberseguridad perfecta es un objetivo difícil de alcanzar, es necesario mitigar los riesgos residuales con medidas destinadas a disminuir las amenazas potenciales.** Estas medidas implican

i. desarticular a los actores de las ciberamenazas,

ii. perseguir más eficazmente los ciberdelitos, y

iii. fomentar la aplicación urgente, a gran escala y efectiva de las normas y reglas existentes, ampliamente acordadas, para el comportamiento de los Estados en el ciberespacio, estableciendo objetivos de actuación compartidos.

También son necesarias asociaciones público-privadas bien diseñadas para el desarrollo normativo y la inversión intersectorial con el fin de apoyar la evolución continua del nivel de protección requerido y, por tanto, la resiliencia de los servicios esenciales y sus cadenas de suministro.

El reto fundamental de la ciberseguridad para proteger los servicios esenciales, las infraestructuras críticas y sus cadenas de suministro puede resumirse en general en tres puntos:

1. **Necesidad de acuerdos transnacionales** para el establecimiento de resultados y objetivos básicos de ciberseguridad. La fragmentación a este nivel no es un enfoque eficaz de la ciberseguridad, sino que más bien crea complejidad, ineficacia y un aumento de los costes que, en última instancia, repercute negativamente en todas las partes interesadas. Los enfoques comunes pueden facilitarse mediante:

   **a.** Alineación en las cadenas de suministro del desarrollo y uso de normativas técnicas de seguridad.

   **b.** Alineación y aplicación de marcos de gestión de riesgos de seguridad basados en el riesgo para los proveedores y operadores de infraestructuras críticas y servicios esenciales.

   **c.** Claridad sobre las funciones y responsabilidades en materia de ciberseguridad en toda la cadena de valor. Los proveedores son responsables de sus productos y soluciones, y los operadores de sistemas críticos son responsables de la ciberseguridad. Los Estados nación son responsables de desarticular a los actores de las ciberamenazas y disminuir las ciberamenazas a las que están expuestos los proveedores y suministradores de infraestructuras y servicios esenciales.

2. **Necesidad de disminuir las ciberamenazas**, incluida la ciberdelincuencia originada por grupos delictivos y las amenazas de Estados o ciberactores patrocinados por Estados.

3. **Identificación de incentivos y elementos disuasorios para la inversión en ciberseguridad** que determinen los núcleos críticos de resiliencia de los servicios esenciales y las infraestructuras críticas, cambiando probablemente la forma en que se diseñan, despliegan y operan dichos servicios e infraestructuras. En la misma línea, también se trataría de cómo se equilibran los objetivos de rentabilidad económica y competencia entre proveedores de servicios con los niveles adecuados de inversión pública en apoyo de la relevancia social de los servicios esenciales y las infraestructuras críticas, más allá de reforzar con regulación el estricto requisito de resiliencia de los mismos.

Ninguno de estos tres puntos puede resolverse con medidas simples o inmediatas.

## Recomendaciones para los agentes del sector privado

Como se señala en las secciones anteriores sobre "buenas prácticas del sector", las empresas ya trabajan para aplicar los controles de seguridad básicos que ayudan a prevenir los ataques y mitigar los riesgos. Estos esfuerzos deben adoptarse y aplicarse a gran escala en todas las regiones y sectores. A modo de recordatorio, las buenas prácticas comunes son:

- Implantar un marco de gestión de riesgos de ciberseguridad para los activos y su cadena de suministro;
- Asegurarse de seguir las recomendaciones de configuración y refuerzo de los proveedores al desplegar los activos en el entorno operativo;
- Mantener un inventario eficaz de los activos y una sólida vigilancia del perímetro con herramientas de gestión de la vulnerabilidad;
- Hacer copias de seguridad periódicas de los datos importantes, almacenados en un sistema debidamente protegido, y realizar pruebas de restauración;
- Prestar atención a las vulnerabilidades de los dispositivos de copia de seguridad y almacenamiento, el software VPN y las puertas de enlace, y aplicar parches al software para solucionar las vulnerabilidades de las aplicaciones de servidor y cliente;
- Establecer un enfoque de confianza cero, siguiendo el principio "nunca confíes, verifica siempre" y en toda la arquitectura de red;
- Utilizar una autenticación multifactor;
- Utilizar sistemas de detección y respuesta de puntos finales (EDR), teniendo en cuenta que la respuesta automatizada puede provocar interrupciones del servicio a menos que esté bien probada en el contexto específico, incluidos los cambios de configuración de EDR y la gestión del ciclo de vida.
- Implantar soluciones avanzadas y automatizadas de detección y respuesta entre capas en todas las plataformas, minimizando al mismo tiempo las repercusiones negativas en la calidad de servicio prevista;
- Emplear firmas antivirus actualizadas y configurar cortafuegos a nivel de aplicación;
- Añadir capacidades de ciberdefensa a los procesos, tecnologías y operaciones;
- Desarrollar planes detallados de respuesta a incidentes (IRP), con procedimientos para las estrategias de respuesta a incidentes y crear un equipo especializado de respuesta a incidentes (IRT);
- Realizar simulacros de crisis a menudo para conocer el nivel de preparación de la organización;
- Impartir formación sobre ciberseguridad para educar a los empleados, realizar auditorías de seguridad periódicas para poner a prueba los mecanismos y minimizar la exposición externa de las redes internas.
- Considerar que la cadena de suministro es clave no sólo para mantener la eficiencia y la calidad del servicio a los clientes, sino también para garantizar que el compromiso potencial de un elemento de la cadena no afecte a otros elementos y al servicio en su conjunto.

## Recomendaciones para los responsables políticos

- Si aún no existe, crear una agencia independiente de ciberseguridad con personal y presupuesto especializados y objetivos y medios específicos, incluida la coordinación periódica de ejercicios cibernéticos.
- Adoptar un enfoque holístico de ciberseguridad pública[70] que i) tenga en cuenta todo el ciclo de vida de los productos y servicios de los que dependen los operadores, ii) reúna a todas las partes interesadas pertinentes y iii) esté coordinado en todo el gobierno y a nivel internacional.
- Dada la creciente complejidad de la cadena de suministro y el ciclo de vida de las redes de comunicación, ninguna parte interesada puede considerarse enteramente responsable de mejorar la seguridad digital en general. Por ello, cuando los gobiernos diseñan políticas para mejorar la seguridad digital de las redes de comunicación, deben tener en cuenta las siguientes cuatro categorías de partes interesadas, que tienen un papel específico en la gestión de los riesgos de seguridad digital:
    - Operadores de redes de comunicación;
    - Usuarios, incluidos los usuarios industriales como los operadores de otras actividades críticas;
    - Proveedores de productos y servicios, incluidos equipos de hardware y software, integración de sistemas, servicios gestionados y servicios en la nube; y
    - Organizaciones de desarrollo de normas (SDO).
- A menudo existe un mosaico de instrumentos legislativos que regulan las obligaciones en materia de ciberseguridad y que afectan a los mismos actores y a diferentes organismos responsables. Un enfoque holístico también incluye la coordinación y la alineación de las demandas entre los diferentes organismos gubernamentales, como el departamento gubernamental encargado de la política de comunicación, el regulador de la comunicación, el regulador de la seguridad digital, la autoridad de competencia, el departamento encargado del desarrollo económico y otros. También es esencial una definición clara de responsabilidades y/o mandatos entre los distintos organismos.
- Desarrollar un plan nacional de seguridad para infraestructuras críticas y servicios esenciales en colaboración con los sectores público y privado.
- Garantizar la transparencia en la designación de infraestructuras críticas y servicios esenciales, trabajando con la industria para determinar cómo deben identificarse las infraestructuras críticas, incluyendo la mitigación de riesgos en la cadena de suministro y los proveedores cubiertos.
- Mejorar las políticas de protección de las cadenas de suministro, incluida la aplicación de normas internacionales y el reconocimiento mutuo de las normas regionales.
- Crear mecanismos de intercambio de información, tanto voluntarios como obligatorios, y garantizar que exista un flujo de información bidireccional.
- Garantizar que las empresas sepan exactamente qué organismos participan no sólo en la regulación de las infraestructuras críticas, sino también en la asistencia en caso de ataque.
- Crear una cultura de ciberseguridad y garantizar el desarrollo de talentos en este ámbito.
- Invertir en la capacitación (incluido el capital humano), la sensibilización y la lucha eficaz contra la ciberdelincuencia.

70 www.oecd-ilibrary.org/science-and-technology/enhancing-the-security-of-communication-infrastructure_bb608fe5-en

## Recomendaciones para una colaboración internacional eficaz

- Es más probable que un marco político nacional holístico sea eficaz si se coordina a nivel internacional, ya que las cadenas de suministro de las redes de comunicación son globales y están interconectadas. Ningún país por sí solo sería capaz de construir desde cero toda la cadena de suministro de productos y servicios críticos para las redes de comunicación. Por lo tanto, los gobiernos deberían:
- Esforzarse por armonizar los enfoques normativos a escala internacional e intersectorial.
- Enumerar los sectores de infraestructuras críticas -por sí mismos y en foros diplomáticos- para incluir sectores tradicionales como el agua, los alimentos o la energía, así como el sector de las TI y, en particular, los servicios en nube que subrayan el mantenimiento y la prestación de servicios esenciales.
- Reconocer en las Naciones Unidas una nueva norma que prohíba los ciberataques patrocinados por el Estado dirigidos contra la cadena de suministro de las TIC.
- Emitir de forma rutinaria declaraciones públicas de atribución tras incidentes cibernéticos llevados a cabo por actores estatales que violen las normas o reglas internacionales, señalando con mayor precisión qué expectativas se violaron.
- Establecer consecuencias disuasorias sólidas para los ciberataques patrocinados por el Estado dirigidos contra infraestructuras críticas que reflejen los costes asociados a la reparación y cualquier daño potencial amenazado por el ataque.

## Recomendaciones para una colaboración público-privada eficaz

- Hacer de la inversión en ciberseguridad parte integrante del plan de desarrollo nacional del gobierno. La rápida digitalización está poniendo a prueba la resiliencia de los servicios e infraestructuras privados y públicos, lo que a su vez significa que la ciberseguridad debe integrarse en la política de modernización de un país. Como mejor práctica, algunos países incluso reservan entre el 10% y el 20% del presupuesto público de apoyo a cada proyecto de transformación digital para la ciberseguridad, con el fin de promover la ciberseguridad desde el diseño. La promoción colaborativa y la financiación de innovaciones tecnológicas en ciberseguridad, en particular el desarrollo y la integración de tecnologías de inteligencia artificial, son cruciales para avanzar en los mecanismos de defensa y contrarrestar eficazmente la creciente frecuencia y sofisticación de los ciberataques. Las medidas para mejorar la ciberseguridad en los proveedores de infraestructuras críticas también podrían fomentarse mediante la aplicación de deducciones fiscales, préstamos con tipos de interés preferentes, subvenciones y otros incentivos.
- Fomentar la cooperación entre las múltiples partes interesadas, incluida la inclusión estructurada de las voces del sector privado y otras partes interesadas en los foros diplomáticos, en las Naciones Unidas y en otros lugares, responsables de establecer y mantener las expectativas internacionales sobre el comportamiento responsable de los Estados en línea.
- Fomentar e incrementar la cooperación internacional entre países y entre actores, rompiendo silos, colaborando con socios privados y haciendo uso de Centros de Operaciones Digitales especializados (SOC/DOC) para agilizar la respuesta en tiempos de crisis.
- Hacer de los requisitos de ciberseguridad un elemento de los contratos públicos.
- Aumentar las medidas de prevención y la capacitación en ciberseguridad.

- Promover el intercambio de información sobre amenazas apoyando los centros de análisis e intercambio de información (ISAC) y los centros de operaciones de seguridad (SOC) regionales. Las plataformas específicas de intercambio de conocimientos podrían ayudar a facilitar el intercambio de lecciones aprendidas, prácticas eficaces e informes detallados sobre ciberataques, mejorando la resiliencia colectiva frente a las amenazas a las infraestructuras críticas.
- Proporcionar financiación a los centros de intercambio de información y aumentar la resiliencia cibernética y la lucha contra la ciberdelincuencia.

# **Anexo I**: Panorama de los enfoques nacionales y regionales sobre la ciberseguridad de las infraestructuras críticas y los servicios esenciales

| Región | País / entidad regional | ¿Cómo se define la infraestructura? | ¿Qué se considera infraestructura crítica? | Fuente |
|---|---|---|---|---|
| **América** | **Argentina** | **En septiembre de 2019, Argentina aprobó una resolución que definió y designó las infraestructuras críticas (IC) y las infraestructuras críticas de información (ICI).**<br><br>*Las Infraestructuras Críticas son **aquellas que resultan esenciales para el correcto funcionamiento de los servicios esenciales** de la sociedad, la salud, la seguridad, la defensa, el bienestar social, la economía y el funcionamiento eficaz del Estado, cuya destrucción o perturbación, total o parcial, las afecta y/o impacta significativamente.*<br><br>*Las ICI son las tecnologías de la información, el funcionamiento y la comunicación, así como la información asociada, que son vitales para el funcionamiento o la seguridad de las IC.* | 1. Energía<br>2. Tecnologías de la información y la comunicación<br>3. Transporte<br>4. Agua<br>5. Salud<br>6. Alimentación<br>7. Finanzas<br>8. Nuclear<br>9. Química<br>10. Espacio<br>11. Estado | Resolución 1523/2019: www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-1523-2019-328599/texto<br><br>Definición y designación en el anexo https://www.argentina.gob.ar/sites/default/files/infoleg/res1523-1-328599.pdf<br><br>Otras definiciones relevantes: https://www.boletinoficial.gob.ar/detalleAviso/primera/216860/20190918 |

| Región | País / entidad regional | ¿Cómo se define la infraestructura? | ¿Qué se considera infraestructura crítica? | Fuente |
|---|---|---|---|---|
| **América** | **Brasil** | El Decreto N° 9.573 del 22 de noviembre de 2018 aprobó la Política Nacional de Seguridad de Infraestructuras Críticas (PNSIC), que define a **las IC como instalaciones, servicios, bienes y sistemas** cuya interrupción o destrucción, total o parcial, tendría un grave impacto social, ambiental, económico, político, internacional o de seguridad para el Estado y la sociedad.<br><br>Asimismo, caracteriza la seguridad de las infraestructuras críticas como un conjunto de medidas preventivas y reactivas destinadas a preservar o restablecer la prestación de servicios relacionados con las IC. | 1. Agua<br>2. Energía<br>3. Transporte<br>4. Comunicaciones<br>5. Finanzas<br>6. Bioseguridad y bioprotección<br>7. Defensa | Política nacional y seguridad de las infraestructuras críticas: www.gov.br/gsi/pt-br/assuntos/seguranca-de-infraestruturas-criticas-sic<br><br>www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm<br><br>Estrategia nacional de seguridad de las infraestructuras críticas: www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10569.htm<br><br>Plan nacional de seguridad de las infraestructuras críticas: www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Decreto/D11200.htm |
| **América** | **Canadá** | Las IC se refieren a procesos, sistemas, instalaciones, tecnologías, redes, activos y servicios esenciales para la salud, la seguridad, la protección o el bienestar económico de los canadienses y el funcionamiento eficaz del gobierno. Las IC pueden ser independientes o estar interconectadas y ser interdependientes dentro y fuera de las provincias, territorios y fronteras nacionales. Las perturbaciones de las IC pueden provocar pérdidas de vidas humanas catastróficas, efectos económicos adversos y un daño significativo a la confianza pública. | 1. Agua<br>2. Seguridad<br>3. Salud<br>4. Finanzas<br>5. Transporte<br>6. Energía y servicios públicos<br>7. Alimentación<br>8. Fabricación<br>9. Gobierno<br>10. Tecnología de la comunicación | Seguridad Pública de Canadá - Infraestructuras críticas de Canadá: www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/cci-iec-es.aspx<br><br>Estrategia nacional para infraestructuras críticas: www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf |

| Región | País / entidad regional | ¿Cómo se define la infraestructura? | ¿Qué se considera infraestructura crítica? | Fuente |
|---|---|---|---|---|
| **América** | **Chile** | Chile aprobó en diciembre de 2023 una Ley Marco de Ciberseguridad e Infraestructuras Críticas de la Información, por la que se crea una agencia nacional de ciberseguridad.<br><br>Ámbito de aplicación de la ley:<br>Requiere a las entidades públicas y privadas que se califiquen como prestadoras de servicios esenciales y a aquellas que, además de prestar Servicios Esenciales, sean calificadas como operadores de vital importancia (OIV) por la nueva Agencia Nacional de Ciberseguridad. | A definir por la nueva Agencia de Ciberseguridad. | Chile Ley Marco de Ciberseguridad e Infraestructuras Críticas de Información: www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=15344&prmBOLETIN=14847-06 (Aprobada en diciembre de 2023) |
| **América** | **Colombia** | Colombia (2022) define la ciberinfraestructura crítica de la siguiente manera: Sistemas y activos, físicos o virtuales, soportados en Tecnologías de la Información y las Comunicaciones, cuya afectación significativa tendría un grave impacto en el bienestar social o económico de los ciudadanos, o en el funcionamiento efectivo del gobierno o la economía.<br><br>**Establece obligaciones de seguridad para las autoridades titulares de infraestructuras críticas o que presten servicios esenciales.** Las autoridades, definidas como titulares de infraestructuras críticas o que prestan servicios esenciales, procurarán disponer de un plan de seguridad digital, protección de redes, ciberinfraestructuras críticas, servicios esenciales y sistemas de información en el ciberespacio y realizarán periódicamente una evaluación de riesgos de seguridad digital.<br><br>Para ello, deben disponer de las normas, políticas, procedimientos, recursos técnicos, administrativos y humanos necesarios para gestionar eficazmente el riesgo, y de conformidad con las mejores prácticas y normas que puedan exigirse. | No hay sectores definidos. | Documento normativo del Gobierno de Colombia sobre infraestructura crítica: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866 |

| Región | País / entidad regional | ¿Cómo se define la infraestructura? | ¿Qué se considera infraestructura crítica? | Fuente |
|---|---|---|---|---|
| **América** | **Estados Unidos de América** | El Instituto Nacional de Normas y Tecnología (NIST) define las infraestructuras críticas como "sistemas y activos, ya sean físicos o virtuales, tan vitales para Estados Unidos que la incapacidad o destrucción de dichos sistemas y activos tendría un impacto debilitador en la seguridad, la seguridad económica nacional, la salud o la seguridad públicas nacionales, o cualquier combinación de estas cuestiones". | 1. Sector químico<br>2. Sector de las instalaciones comerciales<br>3. Sector de las comunicaciones<br>4. Sector manufacturero crítico<br>5. Sector de las presas<br>6. Sector de base industrial de defensa<br>7. Sector de servicios de emergencia<br>8. Sector de la energía<br>9. Sector de los servicios financieros<br>10. Sector agroalimentario<br>11. 11. Sector público<br>12. 12. Sector sanitario y salud pública<br>13. 13. Sector de las tecnologías de la información<br>14. 14. Sector de reactores, materiales y residuos nucleares<br>15. 15. Sector de sistemas de transporte<br>16. 16. Sistemas de agua y aguas residuales | NIST<br>infraestructura crítica - Glosario \| CSRC (nist.gov)<br><br>Agencia de ciberseguridad y seguridad de las infraestructuras – sectores de infraestructuras críticas:<br>Sectores de infraestructuras críticas \| CISA |

| Región | País / entidad regional | ¿Cómo se define la infraestructura? | ¿Qué se considera infraestructura crítica? | Fuente |
|---|---|---|---|---|
| **Asia** | **P. R. China** | El Reglamento de Protección de la Seguridad de las Infraestructuras Críticas de Información (el "Reglamento") fue aprobado en la reunión ejecutiva del Consejo de Estado el 27 de abril de 2021, y entró en vigor el 1 de septiembre de 2021.<br><br>El Reglamento definía las infraestructuras críticas de información como "las instalaciones de red y los sistemas de información clave en sectores e industrias importantes como los servicios públicos de telecomunicaciones e información, la energía, el transporte, la conservación del agua, las finanzas, los servicios públicos, la administración electrónica y la industria científica y tecnológica para defensa nacional, que pueden poner en grave peligro la seguridad nacional, la economía nacional, el sustento de las personas y el bienestar público una vez que son objeto de cualquier destrucción, pérdida de función o fuga de datos". | Importantes instalaciones de red y sistemas de información en sectores importantes, entre ellos:<br><br>1. Sector público de telecomunicaciones y servicios de información<br>2. Sector de la energía<br>3. Sector del transporte<br>4. Sector de la conservación del agua<br>5. Sector financiero<br>6. Servicios públicos<br>7. Sector de la administración electrónica<br>8. Sector de ciencia, tecnología e industria de defensa nacional<br><br>De acuerdo con el SPRCII y la práctica, los operadores de ICI suelen ser informados por las autoridades reguladoras de que las instalaciones de red o los sistemas de información que explotan constituyen ICI, y la lista de dichas ICI no está a disposición del público. | Ley de ciberseguridad de la RPC: www.npc.gov.cn/zgrdw/npc/xinwen/2016-11/07/content_2001605.htm (sólo en chino)<br><br>SPRCII: www.gov.cn/gongbao/content/2021/content_5636138.htm (sólo en chino) |

| Región | País / entidad regional | ¿Cómo se define la infraestructura? | ¿Qué se considera infraestructura crítica? | Fuente |
|---|---|---|---|---|
| **Asia** | **India** | Según la Ley de Tecnología de la Información de 2000 (modificada en 2008), se entiende por ICI "un recurso informático cuya inutilización o destrucción tendrá un impacto debilitador en la seguridad nacional, la economía, la salud pública o la seguridad". | 1. Telecomunicaciones<br>2. Potencia y energía<br>3. Servicios bancarios y financieros<br>4. Transporte<br>5. Entidades estratégicas<br>6. Empresas públicas<br>7. Sanidad | Bank Info Security - La India lanzará un marco de seguridad para infraestructuras críticas: www.bankinfosecurity.asia/india-to-launch-critical-infrastructure-security-framework-a-22282<br><br>Ley de Tecnología de la Información de 2000: eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMjk4NzY=#:~:text=%5B9th%20June%2C%202000%5D%20An,communication%20and%20storage%20of%20information%2C |
| **Asia** | **Singapur** | En virtud del artículo 7(1) de la Ley de Ciberseguridad, una ICI es un ordenador o un sistema informático situado total o parcialmente en Singapur, necesario para la prestación continua de una servicio esencial, y la pérdida o puesta en peligro del ordenador o sistema informático tendrá un efecto debilitador sobre la disponibilidad del servicio esencial en Singapur. | 1. Energía<br>2. Agua<br>3. Banca y finanzas<br>4. Sanidad<br>5. Transporte (terrestre, marítimo y aéreo)<br>6. Infocomm<br>7. Medios de comunicación<br>8. Seguridad y servicio de urgencias<br>9. Gobierno | Panorama de la Ley de Ciberseguridad www.csa.gov.sg/faq/cybersecurity-act<br><br>Cybersecurity Act, Critical Infrastructure: www.csa.gov.sg/legislation/Cybersecurity-Act#:~:text=Los%20sectores%20de%20CII%20son%3A%20Energía,y%20Servicios%2C%20de%20Emergencia%20y%20Gobierno |

| Región | País / entidad regional | ¿Cómo se define la infraestructura? | ¿Qué se considera infraestructura crítica? | Fuente |
|---|---|---|---|---|
| **África** | **Egipto** | La guerra cibernética implica amenazas por parte de naciones y sus grupos patrocinados dirigidas a infiltrarse en los sectores de infraestructuras críticas de otros países, como la energía, las telecomunicaciones y la banca, con fines de espionaje, ganancias políticas y estratégicas, o puramente de sabotaje. Es importante señalar que muchos países han declarado abiertamente poseer capacidades cibernéticas ofensivas como medio de autodefensa contra estas amenazas. En el contexto de Egipto, las "infraestructuras críticas" engloban los servicios y activos esenciales cuya interrupción afectaría significativamente a la seguridad nacional, la estabilidad económica, la salud pública o la seguridad. | 1. Sector de las TIC: Incluye redes de telecomunicaciones, cables submarinos y terrestres, torres de comunicaciones, satélites de comunicaciones, centros de control de comunicaciones y proveedores de servicios de telecomunicaciones e Internet.<br>2. Sector de los servicios financieros: Incluye redes y sitios web de bancos, transacciones bancarias, plataformas de pago electrónico, bolsa, sociedades de valores y servicios financieros postales.<br>3. Sector de la energía: Incluye sistemas, redes y estaciones que controlan la producción y distribución de electricidad, petróleo y gas; estaciones de alta presa; centrales nucleares; y otros.<br>4. Sector de servicios de la Administración: Incluye el portal y los sitios web de la administración electrónica, los sitios web de los organismos e instituciones gubernamentales, las bases de datos nacionales -la más importante de las cuales es la base de datos nacional de documentos de identidad- y las redes y sitios web asociados.<br>5. Sector del transporte: Incluye el transporte aéreo, terrestre, marítimo y por Nilo. Abarca todos los sistemas, centros y redes de control de trenes y metros, así como las redes y sistemas de control del tráfico de navegación aérea y marítima.<br>6. Sector de servicios de ayuda sanitaria y de emergencia: Incluye redes de socorro y emergencia, bancos de sangre, sistemas y redes hospitalarios, redes y sitios web de asistencia sanitaria.<br>7. Sector de la información y la cultura: Incluye redes, sistemas y sitios web de servicios de información y radiodifusión. | Estrategia Nacional de Ciberseguridad para Egipto 2023-2027: www.mcit.gov.eg/Upcont/Documents/Publications_1412024000_National_Cybersecurity_Strategy_2023_2027.pdf<br><br>Estrategia Nacional de Ciberseguridad 2017-2021: https://egcert.eg/wp-content/uploads/2023/02/strategy.pdf |

| Región | País / entidad regional | ¿Cómo se define la infraestructura? | ¿Qué se considera infraestructura crítica? | Fuente |
|---|---|---|---|---|
| **África** | **Ghana** | Las ICI consisten en activos (reales o virtuales), redes, sistemas, procesos, información y funciones que son vitales para la nación y cuya incapacidad o destrucción tendría un impacto devastador en la seguridad nacional, la economía, la salud pública o la seguridad. Las ICI pueden comprender una serie de diferentes infraestructuras con interdependencias esenciales y flujos de información crítica entre ellas. La Ley de Ciberseguridad de 2020 (Ley 1038) define una ICI como un sistema informático o una red informática esencial para la seguridad nacional o el bienestar económico y social de los ciudadanos. | 1. Seguridad nacional e inteligencia<br>2. Tecnología de la información y la comunicación<br>3. Banca y finanzas<br>4. Energía<br>5. Agua<br>6. Transporte<br>7. Salud<br>8. Servicios de urgencia<br>9. Gobierno<br>10. Alimentación y agricultura<br>11. Fabricación<br>12. Minería<br>13. Educación | Directiva sobre protección de infraestructuras críticas de información: www.csa.gov.gh/resources/Directive_CII.pdf<br><br>Ley de Ciberseguridad de 2020: www.csa.gov.gh/resources/cybersecurity_Act_2020(Act_1038).pdf |
| **África** | **Sudáfrica** | Requisitos para la declaración de una infraestructura como infraestructura crítica:<br><br>Una infraestructura puede ser declarada infraestructura crítica si<br><br>(a) el funcionamiento de dichas infraestructuras es esencial para la economía, la seguridad nacional, la seguridad pública y la prestación continua de servicios públicos básicos; y<br><br>(b) la pérdida, daño, perturbación o inmovilización de dichas infraestructuras puede perjudicar gravemente a<br><br>(i) (i) el funcionamiento o la estabilidad de la República.<br><br>(ii) el interés público en materia de seguridad y mantenimiento del orden público; y<br><br>(iii) seguridad nacional. | No hay sectores definidos, las infraestructuras críticas se basan en la definición. | Ley de protección de infraestructuras críticas de 2019: https://static.pmg.org.za/Critical_Infra_Protection_Act8of2019.pdf<br><br>Política de ciberseguridad del agua y contexto legislativo del sector del agua y las aguas residuales en Sudáfrica: www.mdpi.com/2071-1050/13/1/291 |

| Región | País / entidad regional | ¿Cómo se define la infraestructura? | ¿Qué se considera infraestructura crítica? | Fuente |
|---|---|---|---|---|
| **Europa** | **Unión Europea** | En Europa, existen dos directivas principales centradas en la protección de la IC y los servicios esenciales, y algunos enfoques especializados como el centrado en el sector financiero, todos aprobados al mismo tiempo para buscar la coherencia.<br><br>La Directiva sobre la capacidad de recuperación de las entidades críticas (RCE) establece la obligación de adoptar medidas específicas para garantizar que los servicios esenciales para el mantenimiento de las funciones vitales de la sociedad o las actividades económicas se presten sin obstáculos en el mercado interior.<br><br>Pasó de activos a entidades críticas que prestan servicios esenciales con la Directiva 2022/2557:<br><br>Las entidades críticas prestan servicios esenciales para mantener las funciones sociales clave, apoyar la economía, garantizar la salud y la seguridad públicas y preservar el medio ambiente".<br><br>Sin embargo, las entidades críticas exactas son definidas por los Estados miembros de la siguiente manera:<br><br>"Los Estados miembros tendrán que identificar las entidades críticas para los sectores establecidos en la Directiva sobre resiliencia de las entidades críticas (RCE) antes del 17 de julio de 2026. Utilizarán esta lista de servicios esenciales para llevar a cabo evaluaciones de riesgos y, a continuación, identificar las entidades críticas. Una vez identificadas, las entidades críticas tendrán que tomar medidas para mejorar su resiliencia". | 1. Sector energético, con servicios como la producción de electricidad y el almacenamiento de energía;<br>2. Sector del transporte, con servicios como la gestión y el mantenimiento de infraestructuras aeroportuarias o ferroviarias;<br>3. Sector bancario, con servicios esenciales como la captación de depósitos y la concesión de préstamos. (Este sector cuenta con una normativa específica adicional sobre ciberseguridad).<br>4. Sector de infraestructuras de mercados financieros, con servicios como la explotación de centros de negociación y de sistemas de compensación;<br>5. Sector sanitario, con distribución, fabricación, prestación de asistencia sanitaria y servicios médicos;<br>6. Sector del agua potable, con suministro de agua potable y distribución de agua potable;<br>7. Sector de aguas residuales, con servicios de recogida, tratamiento y eliminación de aguas residuales;<br>8. Sector de infraestructuras digitales, con servicios como redes y servicios públicos de comunicaciones electrónicas, prestación y explotación del servicio de punto de intercambio de internet, sistema de nombres de dominio, dominio de nivel superior, computación en nube y centro de datos;<br>9. Servicios del sector de la administración pública;<br>10. Sector espacial, con la explotación de servicios de infraestructura terrestre;<br>11. Sector de producción, transformación y distribución de alimentos, con la producción y transformación industrial de alimentos a gran escala, los servicios de la cadena de suministro de alimentos y los servicios de distribución mayorista de alimentos. | Directiva de Resiliencia de Entidades Críticas (CER): www.eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2557<br><br>Directiva (UE) 2022/2555, de 14 de diciembre de 2022, relativa a medidas para un nivel común elevado de ciberseguridad en la Unión. (NIS2) www.eur-lex.europa.eu/eli/dir/2022/2555/oj<br><br>Reglamento (UE) 2022/2554, de 14 de diciembre de 2022, sobre la resiliencia operativa digital en el sector financiero (DORA) www.eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554 |

| Región | País / entidad regional | ¿Cómo se define la infraestructura? | ¿Qué se considera infraestructura crítica? | Fuente |
|---|---|---|---|---|
| **Europa** | **Reino Unido** | No todo dentro de un sector de infraestructuras nacionales se considera "crítico". La definición oficial de CNI del gobierno británico es:<br><br>Aquellos elementos críticos de la infraestructura (es decir, activos, instalaciones, sistemas, redes o procesos y los trabajadores esenciales que los operan y facilitan), cuya pérdida o puesta en peligro podría provocar:<br><br>a) Impacto perjudicial importante en la disponibilidad, integridad o prestación de servicios esenciales -incluidos aquellos servicios cuya integridad, en caso de verse comprometida, podría ocasionar una pérdida significativa de vidas o víctimas-, teniendo en cuenta las repercusiones económicas o sociales significativas; y/o<br><br>b) Impacto significativo en la seguridad nacional, la defensa nacional o el funcionamiento del Estado". | 1. Productos químicos<br>2. Nuclear Civil<br>3. Comunicaciones<br>4. Defensa<br>5. Servicios de emergencia<br>6. Energía<br>7. Finanzas<br>8. Alimentación<br>9. Gobierno<br>10. Salud<br>11. Espacio<br>12. Transporte<br>13. Agua | |

| Región | País / entidad regional | ¿Cómo se define la infraestructura? | ¿Qué se considera infraestructura crítica? | Fuente |
|---|---|---|---|---|
| **Oceanía** | **Australia** | La Estrategia de Resiliencia de las Infraestructuras Críticas 2023 define las infraestructuras críticas como:<br><br>aquellas instalaciones físicas, cadenas de suministro, tecnologías de la información y redes de comunicación que, si se destruyen, degradan o dejan de estar disponibles durante un periodo prolongado, tendrían un impacto significativo en el bienestar social o económico de la nación, o afectarían a la capacidad de Australia para llevar a cabo la defensa nacional y garantizar la seguridad nacional".<br><br>Cada clase de activo de infraestructura crítica se define en la Ley de Seguridad de Infraestructuras Críticas de 2018. Un único activo de infraestructura crítica incluye múltiples partes, como locales, ordenadores y datos, que funcionan conjuntamente como un sistema o una red.<br><br>Si varios componentes funcionan como un único sistema o red que cumple la definición de activo de infraestructura crítica, se consideran un único activo.<br><br>Si los componentes funcionan como sistemas o redes separados que cumplen cada uno la definición de activo de infraestructura crítica, se consideran activos separados". | 1. Comunicaciones<br>2. Servicios y mercados financieros<br>3. Almacenamiento y tratamiento de datos<br>4. Defensa<br>5. Enseñanza superior e investigación<br>6. Energía<br>7. Alimentación y ultramarinos<br>8. Sanidad y medicina<br>9. Tecnología espacial<br>10. Transporte<br>11. Agua y alcantarillado | |

## Acerca de la Cámara de Comercio Internacional

La Cámara de Comercio Internacional (ICC) es la representante institucional de más de 45 millones de empresas en más de 170 países. La misión principal de la ICC es hacer que los negocios funcionen para todos, todos los días, en todas partes. A través de una combinación única de defensa, soluciones y establecimiento de normas, promovemos el comercio internacional, conductas empresariales responsables y un enfoque global de regulación, además de ofrecer servicios de resolución de conflictos de primer nivel en el mercado. Entre los socios de la ICC figuran muchas de las principales compañías del mundo, PyMEs, asociaciones empresariales y cámaras de comercio locales.

33-43 avenue du Président Wilson, 75116 Paris, France
T +33 (0)1 49 53 28 28  E icc@iccwbo.org
www.iccwbo.org  @iccwbo

"Traducido y editado en español con la colaboración de Telefónica".