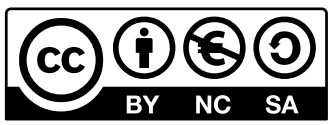
# La seguridad de la infraestructura crítica en América Latina: política, riesgo y resiliencia

DIGI AMERICAS

DIGI AMERICAS ALLIANCE MEMBERS

aws Apple Batuta CHECK POINT CISCO CLOUDFLARE CROWDSTRIKE fluid attacks
Google kriptos LUMU netskope paloalto NETWORKS Resecurity
Schneider Electric SISAP Sistemas Aplicativos SOPHOS tenable Trellix TrendAI whalemate



# Créditos

## Digi Americas Alliance

Alain Karioty
Andy Kotz
Belisario Contreras
Brett DeWitt
Carlos Torales
Christian Torres
Cory Bullock
Federico Nan
Fernando Quintero
Gene Yoo
Ghassan Dreibi
Hernan Armbruster
Jordana Siegel
Jorge Blanco
Marcos Pupo
Mario de la Cruz Sarabia
Mauricio Nanne
Norberto (Bert) Milan
Patrick Ford
Rafael Alvarez
Ricardo Villadiego
Stephen Fallas

## Editores

Belisario Contreras
Andy Kotz

# Índice

# Introducción

La infraestructura crítica (IC) se refiere a diversos sectores y actores que sustentan la estabilidad nacional y el bienestar público. En Estados Unidos, la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) identifica 16 sectores de infraestructuras críticas, incluyendo Energía, Comunicaciones, Servicios Financieros, Sanidad y Salud Pública, Transporte, Agua y Aguas Residuales, y Tecnología de la Información, entre otros.[1] Aunque las clasificaciones varían entre países, los gobiernos latinoamericanos también reconocen las redes energéticas, las redes de telecomunicaciones, los sistemas financieros, los corredores de transporte, los sistemas hídricos y los servicios públicos como fundamentos para el crecimiento económico, la gobernanza democrática y la estabilidad social.[2]

En los últimos años, estos sistemas se han convertido cada vez más en objetivos de operaciones cibernéticas maliciosas llevadas a cabo por grupos criminales, hacktivistas, amenazas internas y actores patrocinados por el Estado. Los actores patrocinados por el Estado, especialmente de China y Rusia, tratan la infraestructura crítica no solo como activos económicos, sino como palanca estratégica en la competencia geopolítica.[3] Las operaciones rusas en Ucrania demuestran que los ciberataques a redes gubernamentales, sistemas de telecomunicaciones e infraestructuras energéticas pueden preceder o acompañar acciones militares, lo que difumina la línea entre la guerra cibernética y la cinética.[4] De manera similar, campañas vinculadas a China como Volt Typhoon y Salt Typhoon han tenido como objetivo los sectores de telecomunicaciones y otras infraestructuras críticas para obtener acceso persistente y sigiloso a las redes, a menudo preposicionándose dentro de los sistemas para permitir posibles interrupciones durante futuras crisis geopolíticas.[5]

Para América Latina, las apuestas siguen siendo especialmente altas. La región está experimentando una rápida transformación digital, ampliando la conectividad, modernizando la infraestructura energética e integrándose cada vez más profundamente en las cadenas de suministro globales. Al mismo tiempo, muchos países se enfrentan a marcos regulatorios desiguales, recursos limitados de ciberseguridad, infraestructuras heredadas y una creciente exposición a amenazas cibernéticas transnacionales. Estos riesgos se ven agravados por la creciente actividad de grupos de amenaza persistente avanzada (APT) vinculados a grandes potencias, que han demostrado la capacidad de infiltrarse y persistir en redes de infraestructura durante largos periodos, a menudo sin ser detectados.[6]

[1] https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors
[2] https://blogs.worldbank.org/en/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe
[3] https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors
[4] https://www.atlanticcouncil.org/blogs/ukrainealert/learning-the-lessons-from-ukraines-fight-against-russian-cyber-warfare/
[5] https://www.congress.gov/crs-product/IF12798
[6] https://www.congress.gov/crs-product/IF12798

Como resultado, la seguridad de infraestructuras críticas va más allá de un simple problema técnico; se sitúa en el centro de la resiliencia nacional, la estabilidad regional y el desarrollo a largo plazo.[7]

Dado que la IC abarca sectores diversos, ningún enfoque único puede garantizarla. Proteger un sistema sanitario requiere medidas diferentes a las que se protegen una central hidroeléctrica o un puerto importante. Un factor clave que distingue la seguridad de la CI de la ciberseguridad tradicional radica en el uso de la tecnología operativa (OT), el hardware y software que monitorizan y controlan los procesos físicos. Los sistemas de control industrial (ICS), que conectan sistemas de tecnología de la información (TI) con entornos OT, generan riesgos que difieren significativamente de las redes TI convencionales. En la mayoría de los países, estos sistemas aún dependen de tecnologías heredadas diseñadas originalmente para la fiabilidad y la continuidad operativa, más que para la ciberseguridad.[8] Al mismo tiempo, la IA ahora transforma tanto la defensa como el ataque: los defensores utilizan la detección de anomalías impulsada por IA para identificar interrupciones sutiles en procesos industriales, mientras que los adversarios pueden usar IA para mapear redes complejas, descubrir vulnerabilidades en sistemas heredados y diseñar estrategias de intrusión más precisas y automatizadas contra entornos OT.[9]

Históricamente, estos sistemas operaban en relativo aislamiento y enfrentaban una exposición limitada a amenazas cibernéticas.[10] Sin embargo, a medida que los operadores de infraestructuras de toda la región adoptan herramientas de monitorización digital, capacidades de acceso remoto y plataformas de gestión en la nube, los sistemas físicos se han vuelto más interconectados y vulnerables. La convergencia de los entornos de TI y OT ha ampliado la superficie de ataque para infraestructuras críticas en los sectores de energía, agua, minería, transporte y telecomunicaciones. Esta superficie de ataque ampliada refleja vulnerabilidades explotadas en Ucrania, donde actores rusos han atacado repetidamente redes eléctricas, redes de comunicaciones y servicios digitales con campañas cibernéticas cada vez más sofisticadas desde 2014.[11] La IA acelera esta situación porque permite ataques más escalables y adaptativos, al tiempo que permite a los defensores desplegar análisis predictivos, respuesta automatizada a incidentes y gemelos digitales para simular y mitigar fallos en cascada en sistemas interconectados.

En todos los sectores, las cadenas de suministro representan un objetivo especialmente atractivo para actores maliciosos. Al comprometer proveedores, proveedores de servicios gestionados o dependencias de software, los adversarios pueden obtener acceso indirecto a activos de infraestructura de alto valor. Estos riesgos no son teóricos.

[7] https://blogs.worldbank.org/en/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe
[8] https://www.cisa.gov/topics/industrial-control-systems
[9] https://red.anthropic.com/2026/mythos-preview/
[10] https://www.cisa.gov/topics/industrial-control-systems
[11] https://www.atlanticcouncil.org/blogs/ukrainealert/learning-the-lessons-from-ukraines-fight-against-russian-cyber-warfare/

En el caso del Volt Typhoon, vinculado a China, las agencias de inteligencia han advertido que los atacantes infiltraron sectores como energía, transporte y sistemas hídricos y mantuvieron el acceso durante años, sugiriendo una estrategia centrada en preposicionarse para posibles interrupciones durante futuras crisis en lugar del espionaje tradicional.[12]

Por tanto, los gobiernos, reguladores, propietarios y operadores de IC, y socios del sector privado en toda América Latina, deben adaptarse a un panorama de amenazas en evolución. Es importante distinguir los roles de los actores dentro de ese ecosistema: los operadores de infraestructuras críticas tienen la responsabilidad directa de proteger los sistemas que operan, mientras que los proveedores tecnológicos, incluidos los proveedores de servicios en la nube, desarrolladores de software y fabricantes de equipos, apoyan esa misión con plataformas seguras, certificadas y transparencia sobre la seguridad de sus productos. En este contexto, la IA debe entenderse no como una solución independiente, sino como un multiplicador de fuerza: su uso efectivo dependerá de los marcos de gobernanza, la calidad de los datos y la experiencia humana, mientras que su mal uso podría reducir la barrera de entrada para operaciones cibernéticas sofisticadas contra infraestructuras críticas. Abordar los riesgos de convergencia TI/OT, fortalecer la seguridad de la cadena de suministro con obligaciones adecuadas al puesto, invertir directamente en el desarrollo de la fuerza laboral y adoptar principios de seguridad por diseño y seguridad por defecto son pasos críticos para construir infraestructuras más resilientes en toda la región.

[12] https://www.theguardian.com/technology/2024/feb/08/chinese-hack-us-transportation-infrastructure

## Identificación y priorización de infraestructuras críticas

Identificar y priorizar correctamente la infraestructura crítica es un paso fundamental para desarrollar estrategias efectivas de ciberseguridad, especialmente en entornos con recursos limitados. Los gobiernos deben primero determinar qué activos y sistemas son más esenciales para la seguridad nacional, la estabilidad económica y la seguridad pública, ya que no toda la infraestructura puede protegerse por igual. Este proceso suele implicar evaluaciones basadas en riesgos que evalúan tanto la probabilidad de interrupción como las posibles consecuencias de un fallo, incluyendo los efectos de desbordamiento en sectores interconectados. En este contexto, los gobiernos también deberían considerar activos menos visibles, pero de gran repercusión. Estos pueden incluir cables de telecomunicaciones submarinos, que transportan la mayor parte del tráfico internacional de datos y son fundamentales para la continuidad económica y la conectividad nacional. A pesar de su importancia, estos activos suelen pasar desapercibidos en los marcos tradicionales de infraestructuras críticas y pueden carecer de medidas adecuadas de protección física y cibernética.

En América Latina, donde las dependencias entre energía, telecomunicaciones, sistemas financieros y redes de transporte están aumentando, la priorización también debe tener en cuenta el riesgo sistémico y las interdependencias intersectoriales. Los escenarios que introducen entornos de riesgo híbridos donde convergen amenazas físicas y cibernéticas, como sistemas aéreos no tripulados (drones) usados para atacar infraestructuras físicas, requieren definiciones ampliadas de lo que constituye infraestructura crítica.

Al definir activos críticos y clasificarlos según su importancia estratégica y vulnerabilidad, los responsables políticos y operadores pueden asignar recursos limitados de forma más eficaz, centrar esfuerzos de mitigación y mejorar la resiliencia general frente a amenazas tanto cibernéticas como físicas. Además, sectores como los servicios espaciales (incluyendo comunicaciones por satélite y GPS), los centros de datos que apoyan infraestructura en la nube y los oleoductos de energía submarina deberían incorporarse mejor a los inventarios nacionales de infraestructuras críticas, ya que su interrupción podría tener impactos desproporcionados y transfronterizos.

## Seguridad en la cadena de suministro

Las cadenas de suministro de infraestructuras críticas son ecosistemas complejos que pueden abarcar cientos de proveedores, integradores, propietarios, operadores y proveedores de servicios.[13] Entre ellos se encuentran fabricantes de hardware, desarrolladores de software,

[13] https://www.energy.gov/ceser/supply-chain-cybersecurity-principles

proveedores de nube, contratistas de mantenimiento, empresas de logística, organismos de certificación y autoridades reguladoras. Estas cadenas de suministro interactúan mediante procesos físicos como la producción y el transporte, así como servicios digitales como la monitorización remota, actualizaciones de software e intercambio de datos.[14]

Uno de los desarrollos más significativos que afectan a infraestructuras críticas y sus cadenas de suministro es la rápida digitalización.[15] Los sistemas de infraestructura dependen cada vez más de componentes impulsados por software, servicios en la nube y conectividad remota. La IA transforma aún más las cadenas de suministro porque permite el mantenimiento predictivo, la toma de decisiones automatizada y la analítica en tiempo real, además de introducir nuevos riesgos relacionados con la integridad de los datos, la seguridad de los modelos y la manipulación adversarial. De cara al futuro, los avances en computación cuántica podrían desafiar los estándares criptográficos actuales que sustentan las comunicaciones seguras a través de cadenas de suministro, lo que genera la necesidad de una planificación a largo plazo en torno al cifrado resistente a la cuántica. Como resultado, la seguridad de un único operador depende ahora de la resiliencia de cada eslabón de su cadena de suministro. Una vulnerabilidad introducida por un proveedor externo de software, proveedor de servicios gestionados o proveedor de equipos puede extenderse a múltiples sectores e incluso a través de fronteras nacionales.

Para gestionar la creciente complejidad, las organizaciones pueden iniciar una reducción significativa de riesgos mediante el establecimiento y la aplicación de estándares mínimos de ciberseguridad para los proveedores. Lo que distingue la ciberseguridad de las cadenas de suministro en el contexto de la IC es su naturaleza colectiva y el hecho de que diferentes actores tienen obligaciones distintas y claramente definidas. Los operadores de infraestructuras críticas mantienen la responsabilidad principal de la seguridad de sus entornos operativos, incluyendo cómo configuran, integran y gobiernan las tecnologías de terceros dentro de esos entornos. Los proveedores tecnológicos como los proveedores de servicios en la nube, los proveedores de servicios de seguridad gestionada y los proveedores de software son responsables de la seguridad de sus plataformas y servicios, lo que normalmente se evidencia a través de certificaciones del sector (ISO 27001, SOC 2, equivalente a FedRAMP), compromisos contractuales y políticas publicadas de responsabilidad compartida. Requisitos de seguridad básicos claros, mecanismos de cumplimiento contractual y supervisión adecuada deberían reflejar esta diferenciación de roles — asegurando la responsabilidad en cada etapa de adquisición, integración y mantenimiento sin desplazar la responsabilidad del operador a proveedores que no controlan cómo se despliegan finalmente sus servicios.

[14] https://www.nics.uma.es/wp-content/papers/Roman2023a.pdf
[15] https://www.nics.uma.es/wp-content/papers/Roman2023a.pdf

La distribución de estas obligaciones de visibilidad debe seguir el control operativo: los operadores de infraestructura son responsables de inventariar sus propios despliegues, configuraciones y dependencias, incluidos los componentes basados en la nube. Los proveedores tecnológicos, a su vez, son responsables de proporcionar la documentación — listas de materiales de software, avisos de seguridad, detalles claros de la arquitectura y pruebas de auditoría — que permiten a los operadores cumplir con sus propias obligaciones de visibilidad. A medida que las cadenas de suministro se amplían para incluir servicios impulsados por IA y, en el futuro, capacidades habilitadas por el sistema cuántico, la transparencia sobre algoritmos, fuentes de datos y dependencias criptográficas será más crítica. Los marcos regulatorios que exigen a los proveedores realizar ejercicios de visibilidad dentro de los entornos del cliente invierten esta lógica y socavan la responsabilidad efectiva.

La monitorización continua, las evaluaciones de riesgos de terceros y las cláusulas de ciberseguridad integradas en los contratos de adquisición traducen compromisos políticos de alto nivel en prácticas operativas. Secure-by-design y secure-by-default deben convertirse en requisitos de contratación, no solo en aspiraciones. Las organizaciones deben incorporar los requisitos de ciberseguridad en los contratos con proveedores con criterios de cumplimiento medibles y establecer una clara rendición de cuentas. Esto incluye la exigencia de que los proveedores muestren prácticas de desarrollo seguras para sistemas de IA y una planificación temprana para la preparación post-cuántica de la criptografía. Para que estas líneas de base sean efectivas a gran escala, los gobiernos y consorcios industriales deben alinearse con marcos estandarizados y políticas de contratación. Iniciativas como el Marco de Ciberseguridad 2.0 del NIST[16] y los principios de seguridad desde el diseño[17] de CISA pueden servir como modelos fundamentales para armonizar las expectativas de los proveedores y hacer cumplir la rendición de cuentas. A medida que la transformación digital se acelera, la superficie de ataque de infraestructuras críticas solo se expandirá. Por lo tanto, fortalecer la seguridad de la cadena de suministro no es solo una necesidad técnica, sino un imperativo estratégico para la resiliencia nacional y la estabilidad económica.

## Convergencia OT/TI y sus implicaciones para la seguridad

A medida que aumenta la integración entre TI y OT, sus medidas de seguridad no deberían funcionar como sistemas aislados. La seguridad informática tradicional enfatiza la tríada de confidencialidad, integridad y disponibilidad (CIA), mientras que la seguridad OT prioriza el funcionamiento continuo y fiable de los procesos físicos y los sistemas de control. Para protegerse frente a una creciente gama de amenazas

[16] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
[17] https://www.cisa.gov/securebydesign

cibernéticas, los entornos OT dependen de sistemas de control supervisado y adquisición de datos (SCADA) y sistemas de control industrial para mantener la resiliencia operativa.[18] La convergencia continua de TI y OT presenta un desafío: alinear las diferentes prioridades de estos ámbitos para garantizar tanto la ciber resiliencia como un rendimiento operativo ininterrumpido en toda la cadena de suministro de infraestructuras críticas.

Las tecnologías emergentes y emergentes aceleran esta convergencia. La IA mejora la detección de amenazas, automatiza la identificación de anomalías y optimiza la eficiencia operativa tanto en entornos de TI como de OT. Sin embargo, estas capacidades también introducen nuevos riesgos, incluyendo el potencial de ataques adversariales a modelos de IA, envenenamiento de datos y una dependencia excesiva de la toma de decisiones automatizada en sistemas críticos para la seguridad. Al mismo tiempo, el impacto futuro de la computación cuántica y otras tecnologías emergentes en el cifrado y las comunicaciones seguras supone un desafío estratégico para los sistemas de TI y OT, especialmente cuando los activos de infraestructura de larga duración dependen de protecciones criptográficas que pueden volverse vulnerables con el tiempo. La preparación para estos cambios requerirá estrategias de seguridad prácticas y visionarias que incorporen la gobernanza de la IA y criptografía cuántica.

Más allá de los resultados técnicos, los procedimientos de respuesta a amenazas y las obligaciones de cumplimiento para TI y OT suelen diferir en la práctica. Los gobiernos y reguladores deben tener en cuenta estas distinciones al elaborar los requisitos futuros y deben distinguir aún más a fondo entre operadores e integradores de infraestructuras críticas —que asumen responsabilidad operativa directa— y proveedores de soluciones tecnológicas como plataformas en la nube o servicios de conectividad, cuyas obligaciones regulatorias deben alinearse con su esfera real de control. Aplicar las obligaciones de los operadores de infraestructuras críticas a proveedores de tecnología que no operan directamente sistemas esenciales distorsionaría la rendición de cuentas y pondría en riesgo la adopción de capacidades avanzadas de seguridad que los operadores con recursos limitados necesitan con urgencia.

# Encuesta a Expertos Regionales

## Antecedentes

Para comprender mejor el ecosistema de ciberseguridad de infraestructuras críticas en América Latina, Digi Americas Alliance realizó una encuesta a 141 partes interesadas de toda la región. Aproximadamente el 46% de los encuestados trabaja en operadores de infraestructuras críticas, mientras que el resto de los participantes representan organizaciones relacionadas involucradas en ciberseguridad, tecnología y políticas. Los encuestados representan a un

[18] https://www.paloaltonetworks.com/cyberpedia/iot-security-vs-ot-security

conjunto diverso de países, incluyendo Colombia (19%), México (14%), Argentina (9%), Panamá (7%) y Ecuador (7%), así como Brasil, Costa Rica, España, Uruguay, República Dominicana, Chile, Estados Unidos, Venezuela, Guatemala, Honduras, Paraguay y Perú.

Los participantes también representan diversos roles dentro de sus organizaciones. Casi la mitad de los encuestados (47%) trabaja en puestos relacionados con la seguridad, mientras que el 21% son miembros de la alta dirección. Otro 19% trabaja en funciones tecnológicas más amplias, mientras que el resto de los encuestados trabaja en áreas como ciberseguridad, gestión general, análisis y ventas. Esta diversidad de roles muestra cómo diferentes grupos interpretan los desafíos de ciberseguridad tal y como se perciben en la dirección organizacional, los equipos técnicos y los grupos de interés operativos.

## Organizaciones

Los encuestados representan organizaciones con estructuras de propiedad variables que operan en múltiples sectores. Aproximadamente el 60% trabaja en organizaciones privadas, el 30% en organizaciones públicas o gubernamentales, y el 10% en organizaciones con estructuras de propiedad mixtas.

Las organizaciones encuestadas también abarcan una amplia gama de sectores que desempeñan papeles clave en las economías nacionales y en los servicios públicos. La mayor proporción de encuestados trabaja en el sector de las tecnologías de la información (24%), seguida de servicios financieros (19%) y servicios gubernamentales (11%). Otros sectores representados incluyen energía (8%), comunicaciones, educación, sanidad y salud pública, agricultura y varias industrias adicionales. Esta diversidad demuestra que la infraestructura crítica abarca múltiples sectores y que los riesgos pueden desplazarse de un sector a otro.

## Resultados de la encuesta

Fig. 1 — ¿Su organización cuenta con una estrategia de ciberseguridad documentada?

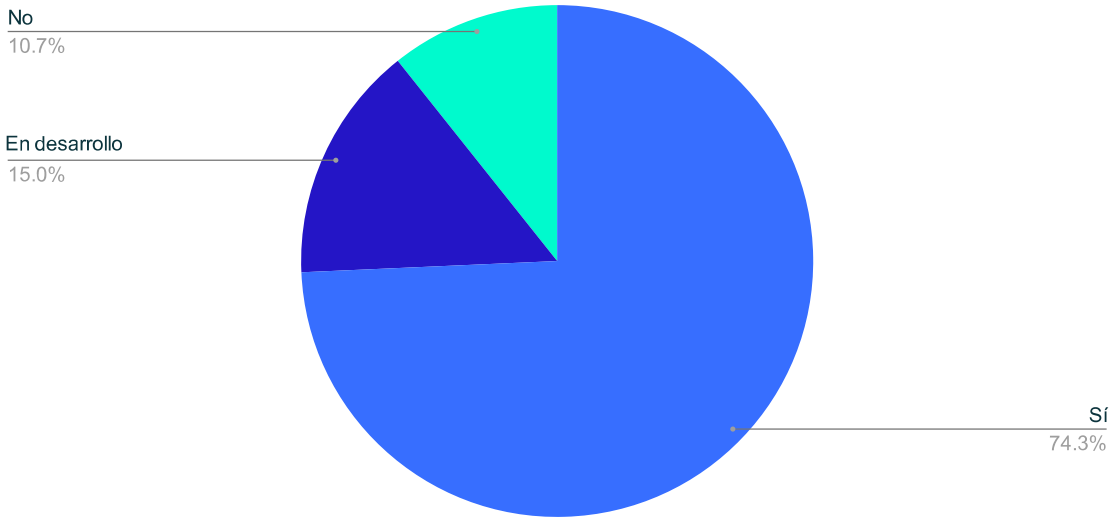



Fig. 2 — ¿Su organización cuenta con una estrategia dedicada a OT o incluye OT en su estrategia de ciberseguridad?

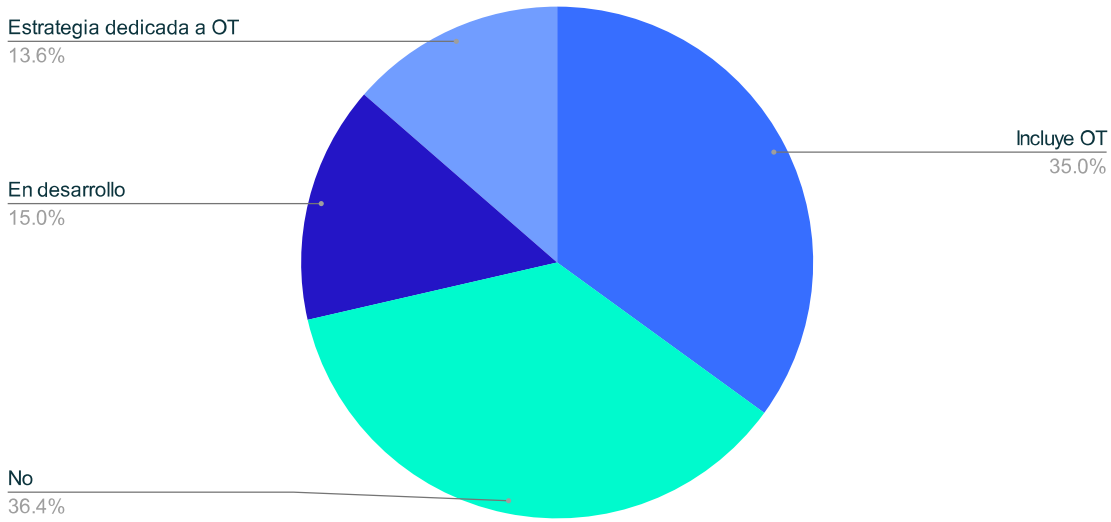


Fig. 3 — ¿Su organización depende de prácticas de seguridad de TI para proteger entornos OT?

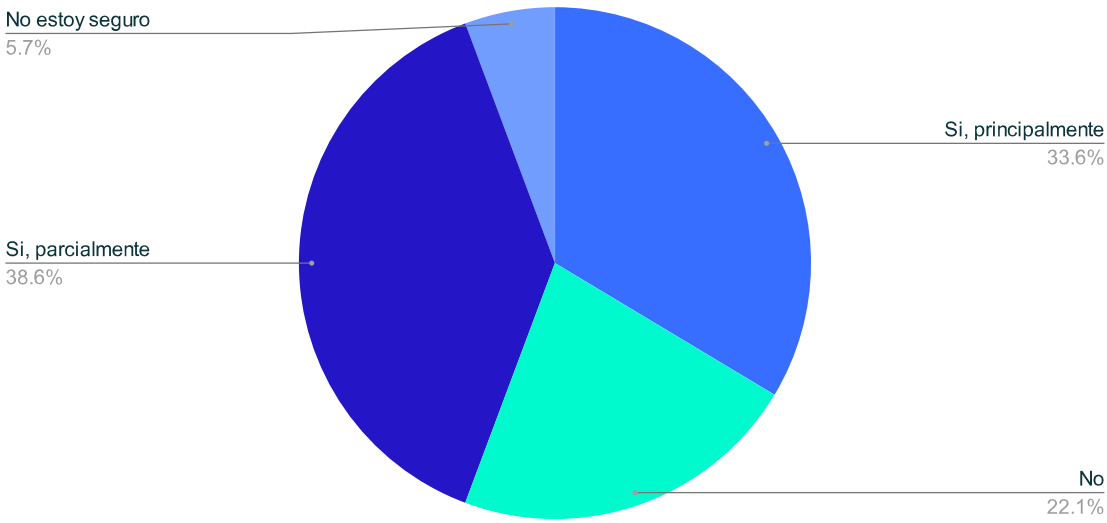
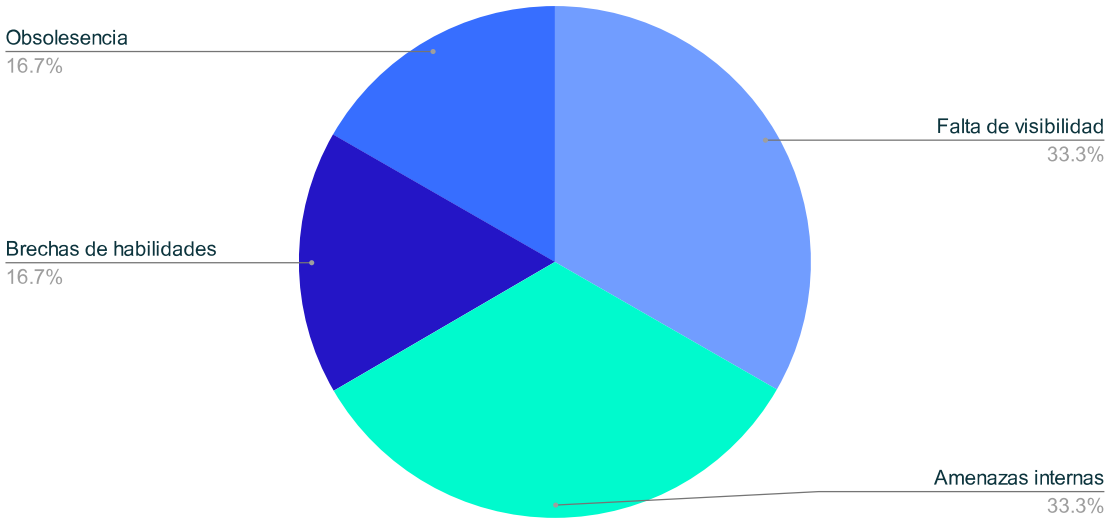



Fig. 4 — ¿Cuáles son sus principales desafíos para proteger datos sensibles y regulados en TI/OT?




Uno de los pasos más importantes para las organizaciones, especialmente aquellas designadas como infraestructura crítica, es establecer un plan claro para proteger tanto sus activos operativos de tecnología (OT) como sus activos de tecnología de la información (TI). La Figura 1 muestra que la mayoría de las organizaciones (90%) tienen una estrategia de ciberseguridad documentada o están desarrollando una activamente. Sin embargo, la Figura 2 indica que la mayoría (51%) de estas mismas organizaciones no tienen actualmente un plan que haga referencia explícita a OT, lo que señala una brecha crítica que debe abordarse. Proteger los sistemas físicos requiere planes deliberados que aborden los riesgos específicos asociados a los entornos de terapia ocupacional. La Figura 3 destaca además que la mayoría de las organizaciones (72%) dependen al menos parcialmente de las prácticas de seguridad informática para proteger los sistemas OT. Aunque TI y OT comparten algunas similitudes, implican requisitos operativos y perfiles de riesgo fundamentalmente diferentes y, por tanto, requieren estrategias y prácticas de seguridad distintas.

Fig. 5 — ¿Su organización está utilizando actualmente IA o aprendizaje automático para fines de ciberseguridad?

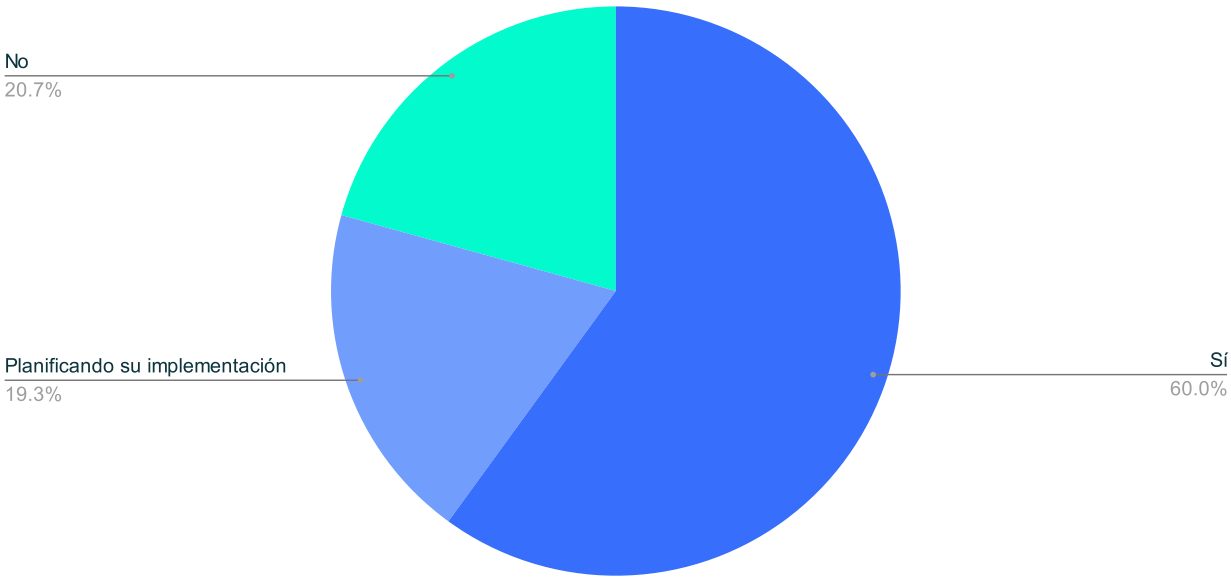



Fig. 6 — ¿Su organización ha desarrollado y aplicado políticas de uso de IA para uso interno y proveedores?

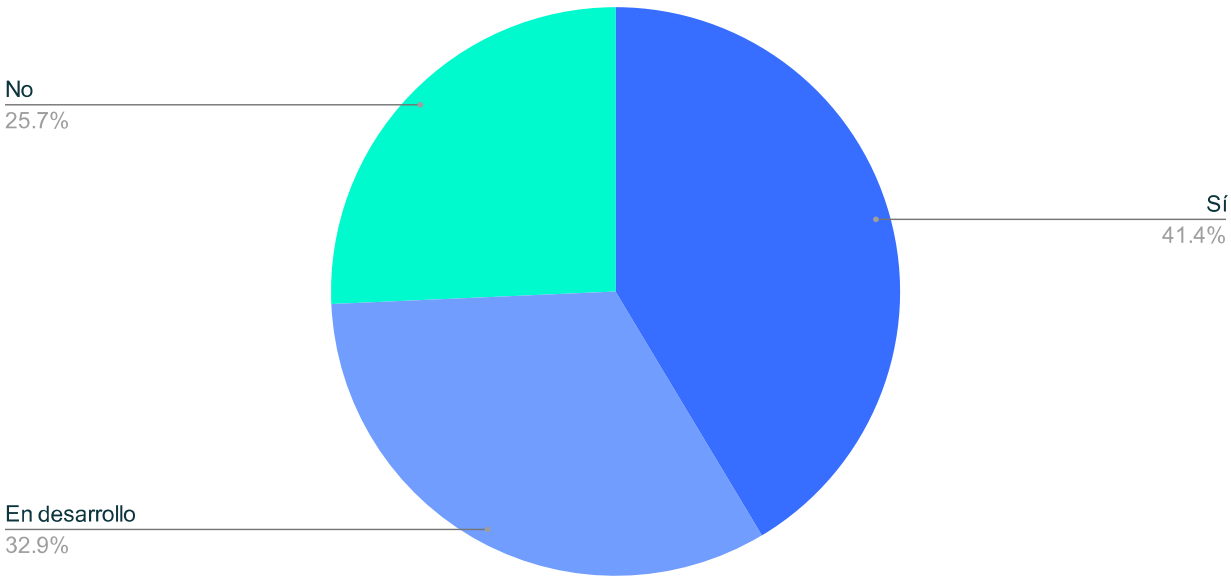


Fig. 7 — ¿Qué tan preparada considera que está su organización para enfrentar amenazas cibernéticas impulsadas por IA

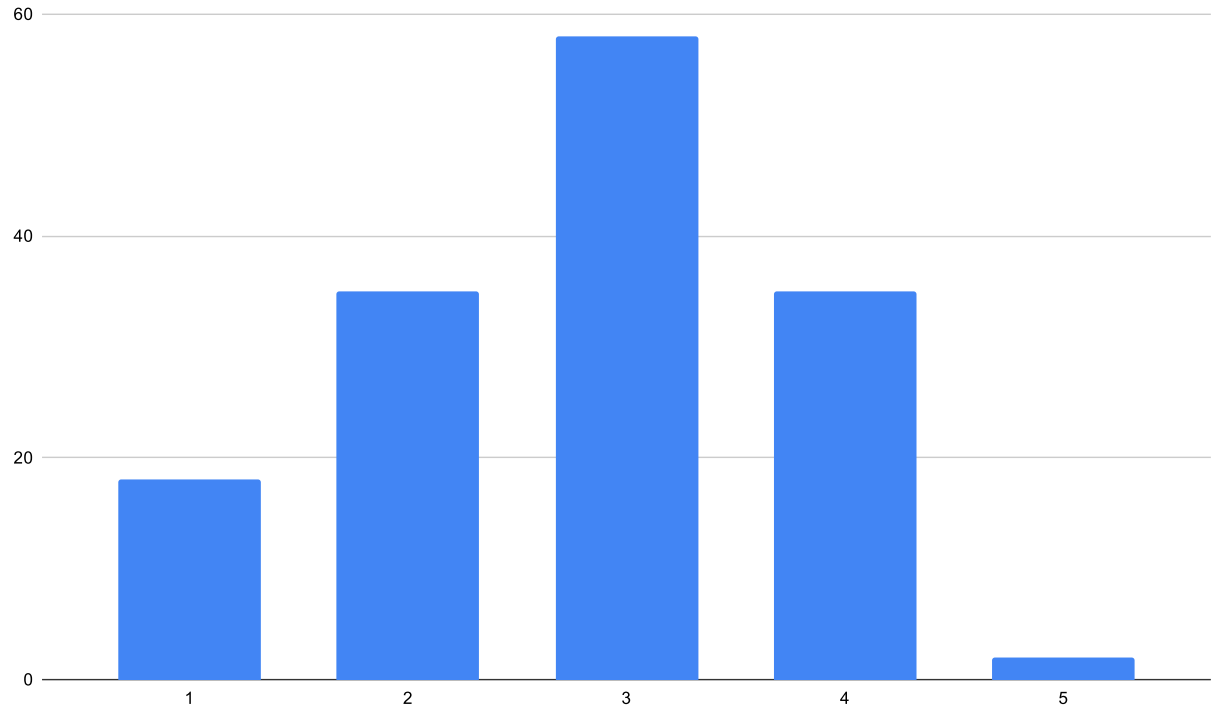
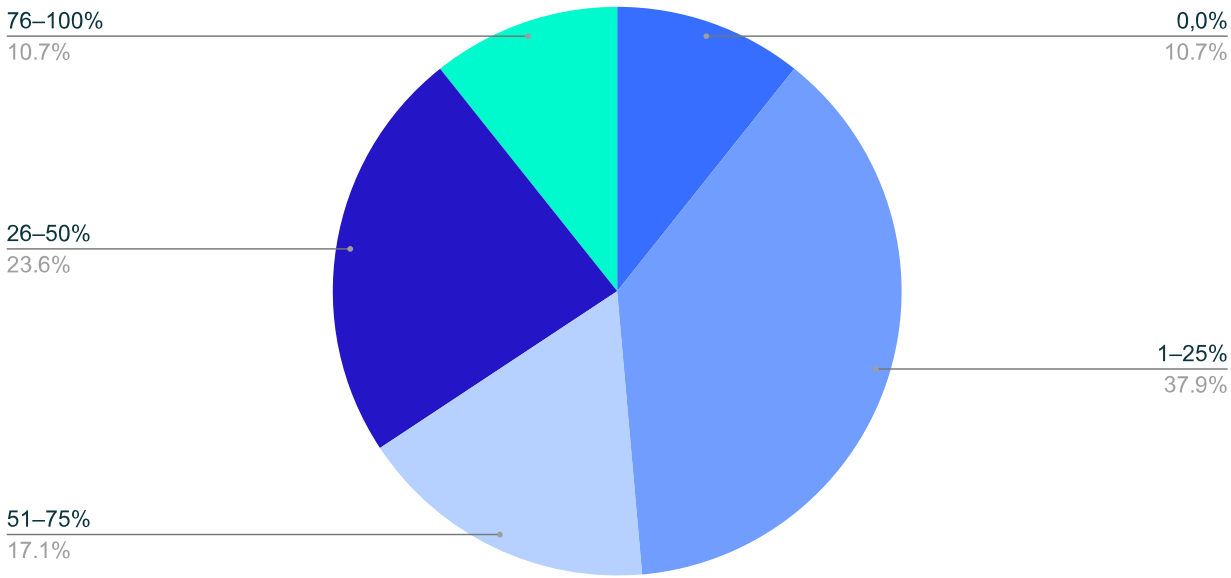



Fig. 8 — ¿Qué porcentaje de sus sistemas críticos (TI/OT) funcionan actualmente en infraestructura en la nube?



Las figuras 5 y 6 destacan el creciente papel de la inteligencia artificial en las operaciones de ciberseguridad dentro de las organizaciones de infraestructuras críticas. Aproximadamente el 80% de los encuestados informó que sus organizaciones utilizan activamente IA en sistemas de ciberseguridad (60%) o están planificando su implementación (19%). Esto sugiere que la IA ya está teniendo un impacto significativo en las operaciones de ciberseguridad, especialmente en áreas como la detección de amenazas, la monitorización y la automatización. Sin embargo, a pesar de esta adopción generalizada, alrededor del 25% de las organizaciones informan que no tienen una política formal de IA que regule ni el uso interno ni los proveedores externos. A medida que la IA continúa evolucionando e integrándose más en entornos de ciberseguridad, será esencial establecer políticas claras para gestionar tanto los beneficios como los riesgos potenciales asociados a su uso.

La Figura 7 destaca el otro lado del creciente papel de la IA en la ciberseguridad: la aparición de amenazas nuevas y más sofisticadas. La IA introduce tanto capacidades defensivas como nuevos vectores de ataque. Por ello, las organizaciones deben abordar la seguridad de la IA en tres dimensiones: IA para la seguridad (usando IA para detectar anomalías y automatizar la respuesta a amenazas), seguridad para la IA (para proteger los sistemas de IA de ataques adversarios) y gobernanza de la IA (para establecer políticas de uso responsable de la IA). Cuando se les preguntó qué tan preparada estaba su organización para manejar amenazas cibernéticas impulsadas por IA, como deepfakes o malware generado por IA, casi ningún encuestado indicó sentirse "muy preparado". La mayoría de los encuestados eligió un nivel de preparación moderado (3), y muchos otros eligieron niveles de preparación más bajos (2) o algo más altos (4). Estas respuestas muestran que, aunque las organizaciones adoptan cada vez más la IA como herramienta defensiva, muchas aún se sienten inseguras sobre su capacidad para contrarrestar ataques habilitados por IA. Dado que las capacidades de IA continúan avanzando, es crucial mejorar la preparación organizativa para hacer frente a estas amenazas, que serán cada vez más importantes.

## Seguridad en la nube

La infraestructura en la nube ofrece ventajas críticas que protegen mejor la tecnología operativa y los sistemas de infraestructura crítica que los entornos locales que pueden igualar. Para las organizaciones latinoamericanas con recursos limitados que se enfrentan a amenazas sofisticadas patrocinadas por el Estado, la adopción de la nube transforma la ciberseguridad de una carga costosa que requiere inversión constante en una capacidad compartida que mejora con la escala. Esto lo hace más seguro como imperativo estratégico para proteger infraestructuras críticas y, al mismo tiempo, permite la transformación digital.

La Figura 8 destaca hasta qué punto los sistemas de infraestructuras críticas operan actualmente en entornos cloud. Los resultados muestran que la mayoría de las organizaciones han comenzado a integrar tecnologías en la nube en sus operaciones, aunque normalmente de forma limitada. La mayor proporción de

encuestados (37,9%) informó que entre el 1 y el 25% de sus sistemas críticos (TI/OT) operan actualmente en la nube. Otro 23,6% indicó que entre el 26 y el 50 % de sus sistemas funcionan en entornos en la nube, mientras que porciones menores reportaron mayores niveles de adopción, incluyendo un 17,1 % con el 51–75 % de los sistemas en la nube y el 10,7 % con un 76–100 %. Solo una pequeña proporción de los encuestados informó de no usar la nube o de una adopción muy mínima.

Estos resultados sugieren que, aunque las tecnologías en la nube se trasladan a entornos de infraestructuras críticas, muchas organizaciones siguen adoptando un enfoque cauteloso, especialmente en lo que respecta a los sistemas tecnológicos operativos que tradicionalmente han permanecido en las instalaciones. A medida que la adopción en la nube se expande, las organizaciones deben asegurarse de que los controles de seguridad adecuados, la visibilidad y los marcos de gobernanza protejan los activos de TI y OT en entornos híbridos y basados en la nube.

# Mejores prácticas

Los resultados de la encuesta indican que los gobiernos, la industria y otros actores deben actuar. Aunque muchos países de la región aún están desarrollando políticas y marcos regulatorios para abordar la seguridad de infraestructuras críticas, varios gobiernos e instituciones en todo el mundo ya han comenzado a implementar estrategias, estándares y directrices diseñadas para fortalecer la resiliencia de las infraestructuras críticas y los sistemas industriales. Estos esfuerzos demuestran una variedad de enfoques, incluyendo la integración de la seguridad de OT en las estrategias nacionales de ciberseguridad, el desarrollo de marcos dedicados a OT, el fortalecimiento de la seguridad de la cadena de suministro y el establecimiento de requisitos regulatorios regionales para sectores críticos.

La siguiente sección destaca una selección de estas mejores prácticas tanto dentro como fuera de la región. Al mostrar iniciativas existentes, la sección pretende ofrecer a responsables políticos, reguladores y operadores del sector privado ejemplos prácticos de cómo gobiernos y organizaciones están abordando riesgos críticos de ciberseguridad. Estos modelos ofrecen lecciones que pueden ayudar a los países a desarrollar o perfeccionar sus propios marcos, promover una colaboración público-privada más fuerte y establecer estándares consistentes para proteger los sistemas que sustentan los servicios esenciales y la infraestructura crítica.

## Brasil

### Estrategia Nacional de Ciberseguridad

La Estrategia Nacional de Ciberseguridad de Brasil (E-Ciber) enfatiza la protección de infraestructuras críticas y servicios esenciales, como energía, telecomunicaciones, sanidad y otros sectores estratégicos, que dependen

en gran medida de sistemas OT.[19] La estrategia prioriza la mejora de la seguridad y la resiliencia de las infraestructuras críticas, la promoción de la gestión de riesgos, la prevención de incidentes y una coordinación más fuerte entre el gobierno y el sector privado para prevenir y responder a incidentes cibernéticos que afectan a estos sistemas.

Al vincular explícitamente la política de ciberseguridad con la protección de servicios e infraestructuras esenciales, la estrategia de Brasil también aborda la seguridad de los entornos OT que sustentan estos sectores. Este enfoque ofrece una lección útil para otros países de la región y demuestra que las estrategias nacionales de ciberseguridad no deben centrarse únicamente en los sistemas informáticos, sino también incorporar la protección de los sistemas industriales y operativos que apoyan infraestructuras críticas. Integrar la seguridad de las OT en marcos nacionales más amplios de gobernanza cibernética puede ayudar a los gobiernos a fortalecer la resiliencia, fomentar la colaboración público-privada y promover estándares de seguridad coherentes en sectores críticos.

## Colombia

### Estrategia Nacional de Seguridad Digital 2025-2027

La Estrategia Nacional de Seguridad Digital 2025–2027 de Colombia se basa en la base establecida por CONPES 3995 (2020) y adopta un enfoque más operativo y enfocado en la implementación de la ciberseguridad, con un fuerte énfasis en la protección de infraestructuras críticas y servicios esenciales.[20] [21] La estrategia prioriza la seguridad y la resiliencia de las infraestructuras cibernéticas críticas, reconociendo su papel central en el apoyo a sectores como la energía, las finanzas, la sanidad y los servicios gubernamentales.

Un elemento clave de la estrategia es su énfasis en la ciber resiliencia y la gestión de riesgos. Promueve la identificación proactiva de vulnerabilidades, la monitorización continua y capacidades más sólidas de detección y respuesta a incidentes tanto en operadores públicos como privados. El marco también enfatiza la preparación para incidentes cibernéticos a gran escala, incluyendo mecanismos nacionales coordinados de respuesta y mejores capacidades de recuperación para los servicios esenciales. Además, la estrategia fortalece la gobernanza institucional y el fortalecimiento de capacidades, abordando las lagunas identificadas en marcos anteriores. Incluye esfuerzos para mejorar las capacidades nacionales de ciberdefensa, ampliar el desarrollo de la fuerza laboral y alinear las iniciativas de ciberseguridad con objetivos más amplios de desarrollo nacional y transformación digital.

El enfoque de Colombia ofrece una lección clave para la región: fortalecer la resiliencia de infraestructuras críticas requiere no solo controles técnicos, sino también estructuras de gobernanza bien definidas

[19] https://www.in.gov.br/en/web/dou/-/decreto-n-12.573-de-4-de-agosto-de-2025-646200784
[20] https://www.mintic.gov.co/portal/715/articles-403023_recurso_2.pdf
[21] https://depp.oecd.org/policies/COL2168

y capacidades nacionales coordinadas. La integración de la ciberseguridad en marcos digitales más amplios de confianza y gestión de riesgos puede mejorar la capacidad de los países para gestionar mejor las amenazas a los entornos informáticos y operativos que apoyan servicios esenciales.

## Unión Europea

### Directiva 2022/2555 - NIS2

La Directiva 2 de la Unión Europea sobre Seguridad de la Información y la Redes (NIS2) establece uno de los enfoques regulatorios más completos para la ciberseguridad en infraestructuras críticas.[22] Adoptada en 2022 y sustituyendo a la Directiva original de la NIS, la NIS2 establece un marco legal común para la ciberseguridad entre los Estados miembros de la UE, que abarca organizaciones que operan en 18 sectores críticos como energía, transporte, sanidad, finanzas e infraestructura digital. La directiva obliga a las entidades públicas y privadas consideradas "esenciales" o "importantes" a implementar medidas de gestión de riesgos, mejorar la gobernanza y las capacidades de respuesta a incidentes, y a reportar incidentes cibernéticos significativos a las autoridades nacionales dentro de plazos definidos.[23]

La directiva tiene claras implicaciones para la tecnología operativa y la infraestructura ciberfísica, ya que muchos sectores cubiertos dependen en gran medida de sistemas de control industrial y otros entornos OT. Al imponer controles de seguridad básicos, gestión de riesgos en la cadena de suministro y responsabilidad a nivel ejecutivo en ciberseguridad, NIS2 mejora la resiliencia global de las infraestructuras críticas en toda la UE.[24]

Este modelo ofrece una lección útil para otras regiones: establecer requisitos armonizados de ciberseguridad para sectores críticos a nivel regional puede ayudar a estandarizar protecciones, mejorar la cooperación transfronteriza y garantizar que tanto los sistemas de TI como los OT que apoyan los servicios esenciales estén protegidos frente a las amenazas cibernéticas en evolución.

## México

### Plan Nacional de Ciberseguridad 2025-2030

El Plan Nacional de Ciberseguridad de México 2025–2030[25] supone un cambio significativo hacia un modelo de ciberseguridad más centralizado, preventivo y centrado en la infraestructura. Desarrollado por la Agencia para la Transformación Digital y las Telecomunicaciones (ATDT), el plan representa la primera política integral y intersectorial de ciberseguridad del país y prioriza la protección de infraestructuras críticas y servicios esenciales como objetivo nacional central.[26]

[22] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555
[23] https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
[24] https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
[25] https://www.gob.mx/atdt/comunicacion/liderara-mexico-ciberresiliencia-en-la-region-con-plan-nacional-de-ciberseguridad
[26] https://mexicobusiness.news/cybersecurity/news/mexico-unveils-national-cybersecurity-plan-2025-2030

Un componente central del plan es la creación de una gobernanza unificada y una arquitectura operativa que sustituya esfuerzos históricamente fragmentados. Esto incluye el establecimiento de un Centro Nacional de Operaciones de Ciberseguridad (CNSOC) para la monitorización en tiempo real, un centro federal de respuesta a incidentes (CSIRT) y un inventario nacional de infraestructuras críticas para identificar y priorizar la protección de activos estratégicos en sectores como energía, finanzas, telecomunicaciones y sistemas gubernamentales.[27] Estas medidas se complementan con un sistema de evaluación y alerta de vulnerabilidades diseñado para identificar y remediar de forma proactiva las debilidades en los sistemas del sector público.[28]

El plan también introduce estándares obligatorios de ciberseguridad, requisitos de notificación de incidentes y marcos de gestión de riesgos para entidades federales, lo que señala un avance hacia protecciones más exigibles y estandarizadas para infraestructuras críticas. Paralelamente, México pretende fortalecer la coordinación entre gobierno, industria y academia a través de un Consejo Nacional de Ciberseguridad y mecanismos ampliados de intercambio de información, reconociendo que la resiliencia de infraestructuras depende de la colaboración entre múltiples partes interesadas.[29]

El enfoque de México ofrece una lección importante para la región: la transición de esfuerzos fragmentados en ciberseguridad a un marco centralizado y orientado a políticas —con instituciones dedicadas, estándares obligatorios y un inventario nacional de infraestructuras críticas— puede mejorar significativamente la visibilidad, coordinación y resiliencia. Al mismo tiempo, el caso mexicano subraya la necesidad de complementar las reformas de gobernanza de alto nivel con orientación sectorial y técnica, especialmente para entornos de OT que sustentan infraestructuras críticas.

## Singapur

### Plan Director de Ciberseguridad en Tecnología Operativa 2024

Singapur ha adoptado un enfoque dirigido para la seguridad de la tecnología operativa (OT) a través de su Plan Director de Ciberseguridad en Tecnología Operativa 2024, publicado por la Agencia de Ciberseguridad de Singapur (CSA).[30] El plan actúa como un plan nacional para fortalecer la postura de ciberseguridad de las organizaciones que operan sistemas de TO tanto en sectores de infraestructura de información crítica (CII) como en otras industrias dependientes de OT. Se centra en fortalecer las capacidades en tres pilares (personas, procesos y tecnología), incluyendo la expansión de la cartera de talento en ciberseguridad OT, una mejor

[27] https://nearshoreamericas.com/mexico-moves-to-strengthen-cybersecurity-with-new-national-plan-and-law/
[28] https://blog.knowbe4.com/mexico-unveils-its-first-national-cybersecurity-plan-a-new-era-of-digital-resilience
[29] https://www.eleconomista.com.mx/tecnologia/gobierno-sheinbaum-presenta-plan-nacional-ciberseguridad-2025-20251204-789652.html
[30] https://www.csa.gov.sg/resources/publications/singapore-s-operational-technology-cybersecurity-masterplan-2024/

compartición de información e informes de incidentes, resiliencia más allá de los sectores tradicionales de infraestructuras críticas y el uso de principios de seguridad por despliegue y seguridad por diseño a lo largo del ciclo de vida de los sistemas OT.[31]

El enfoque de Singapur ofrece una lección importante para otras regiones: en lugar de tratar la seguridad OT únicamente como un subconjunto de la política general de ciberseguridad, los gobiernos pueden desarrollar marcos nacionales dedicados para sistemas OT que aborden el desarrollo de la fuerza laboral, la coordinación sectorial y la seguridad a lo largo de vida de las tecnologías industriales. Al integrar agencias gubernamentales, actores industriales e instituciones educativas en una estrategia coordinada, Singapur demuestra cómo los países pueden fortalecer proactivamente la resiliencia de las infraestructuras críticas y los sistemas físicos emergentes.[32]

## Estados Unidos de América

### Principios de ciberseguridad de la cadena de suministro del Departamento de Energía (DOE)

En 2024, la Oficina de Ciberseguridad, Seguridad Energética y Respuesta a Emergencias (CESER) del Departamento de Energía de EE. UU. (DOE) publicó un conjunto de principios de ciberseguridad en la cadena de suministro para apoyar a proveedores y usuarios finales con el fin de proteger la cadena de suministro, con un enfoque específico en el sector energético.[33] Los principios abarcaban los siguientes conceptos y objetivos de ciberseguridad:

- Gestión de riesgos orientada al impacto
- Defensas informadas por marcos
- Fundamentos de la ciberseguridad
- Desarrollo e implementación seguros
- Transparencia y construcción de confianza
- Orientación de implementación
- Soporte y mantenimiento durante el ciclo de vida
- Gestión proactiva de vulnerabilidades
- Respuesta proactiva a incidentes
- Resiliencia empresarial y operativa

El documento también enfatiza que la seguridad es una responsabilidad compartida y que la colaboración es absolutamente necesaria a lo largo de una cadena de suministro compleja. Por ejemplo, el documento destaca que "los proveedores de tecnología energética pueden obtener subcomponentes de cientos de fabricantes diferentes para un solo equipo; esa tecnología puede ser adquirida por otro proveedor e integrada en un sistema adicional antes de llegar al usuario final." Para que los usuarios finales tengan confianza en sus sistemas, deben confiar en que toda la cadena de suministro sigue los mismos principios de seguridad.[34]

[31] https://www.csa.gov.sg/resources/publications/singapore-s-operational-technology-cybersecurity-masterplan-2024/
[32] https://www.rajahtannasia.com/viewpoints/singapore-launches-updated-national-operational-technology-cybersecurity-masterplan/
[33] https://www.energy.gov/ceser/supply-chain-cybersecurity-principles
[34] https://www.energy.gov/ceser/supply-chain-cybersecurity-principles

### NIST SP 800-82 Rev. 3: Guía de Seguridad en Tecnología Operativa (OT)

En 2023, el NIST publicó el SP 800-82 Rev. 3: Guía para la Seguridad en Tecnología Operativa (OT).[35] El documento ofrece una guía completa sobre cómo proteger OT, "al tiempo que aborda sus requisitos únicos de rendimiento, fiabilidad y seguridad."[36] Además de una explicación sobre la OT, la seguridad de las OT y cómo la OT encaja en diferentes entornos de sistema, el documento también ofrece una visión general de "OT" y las topologías típicas de sistemas, identifica amenazas y vulnerabilidades comunes a estos sistemas, y enumera las contramedidas de seguridad recomendadas para mitigar los riesgos asociados.

La guía establece un enfoque basado en riesgos para proteger entornos OT, incluyendo mejores prácticas como estrategias de defensa en profundidad, evaluaciones regulares de riesgos y vulnerabilidades, y procesos robustos de respuesta y recuperación a incidentes. También vincula las prácticas de ciberseguridad en TO con marcos más amplios como el Marco de Ciberseguridad del NIST y los controles de seguridad NIST SP 800-53, que permiten a las organizaciones incluir la seguridad OT en programas de gestión de riesgos a nivel empresarial.[37]

## Recomendaciones

Una regulación eficaz de la ciberseguridad debería diferenciar las obligaciones entre los operadores de infraestructuras críticas y los proveedores de soluciones tecnológicas mediante un marco de responsabilidad compartida. Los operadores de infraestructuras críticas —entidades que operan directamente sistemas esenciales como redes energéticas, sistemas de agua o redes de telecomunicaciones— tienen la responsabilidad principal de proteger sus entornos operativos, incluyendo evaluaciones de riesgos, respuesta a incidentes y controles de seguridad apropiados a sus operaciones. Los proveedores de soluciones tecnológicas como los proveedores de servicios en la nube, las redes de distribución de contenidos y los servicios de almacenamiento de datos mantienen la seguridad de sus plataformas y servicios mediante certificaciones del sector y obligaciones contractuales, mientras que los operadores mantienen la responsabilidad de la seguridad en el uso de esos servicios, incluyendo las decisiones de configuración y control de acceso.

Las regulaciones deben reconocer explícitamente el Principio de Responsabilidad Compartida y distribuir las obligaciones de prevención, protección, respuesta y recuperación entre los actores públicos y privados de sistemas digitales, según su función específica, nivel de exposición y capacidad operativa.

[35] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf
[36] https://csrc.nist.gov/pubs/sp/800/82/r3/final
[37] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf

Este enfoque basado en riesgos y neutral tecnológicamente garantiza que la responsabilidad esté alineada con el control operativo real, permite a los operadores de infraestructuras elegir proveedores en función de sus capacidades de seguridad en lugar de la clasificación regulatoria, y promueve un entorno regulatorio que mejora la seguridad y permite la transformación digital y el acceso a capacidades avanzadas de seguridad en la nube.

Aprendiendo de la encuesta y de las mejores prácticas, el artículo ofrece las siguientes recomendaciones.

## Plan para la Seguridad de OT

Las organizaciones responsables de infraestructuras críticas deben establecer una responsabilidad clara en la seguridad de la tecnología operativa (OT). Ya sea que la seguridad de las OT se gestione dentro de un equipo de ciberseguridad IT existente o a través de una función dedicada a la seguridad de OT, debe haber personal específicamente encargado de proteger los sistemas de control industrial y los activos relacionados. Sin una propiedad definida, las iniciativas de ciberseguridad en OT a menudo pierden prioridad y pasan desapercibidas, dejando los sistemas críticos expuestos a riesgos prevenibles. Establecer liderazgo, responsabilidad y una estrategia formal garantiza que los entornos de OT reciban atención, recursos y gestión de riesgos de forma consistente.

## Mapeo de la Convergencia de TI/OT

A medida que los sistemas de TI y OT se interconectan cada vez más, las organizaciones deben mapear claramente cómo interactúan estos entornos. Históricamente, los sistemas industriales estaban aislados, pero la modernización y la transformación digital han introducido nuevos puntos de conectividad y posibles vulnerabilidades. Una visión clara de dónde interactúan las redes de TI y OT permite a las organizaciones identificar riesgos, aclarar responsabilidades de gobernanza e implementar controles de seguridad apropiados. La convergencia de mapeo también permite una mejor coordinación entre los equipos de TI y OT, asegurando que las políticas, la monitorización y los procesos de respuesta a incidentes tengan en cuenta las realidades de los entornos integrados.

## Asegurar la cadena de suministro

La ciberseguridad para infraestructuras críticas debe extenderse más allá de los operadores individuales para incluir toda la cadena de suministro. Los gobiernos y los operadores de infraestructuras deberían exigir estándares básicos de OT y ciberseguridad informática por parte de proveedores, fabricantes, integradores y proveedores de servicios. Dado que diferentes actores interpretan distintos papeles, los requisitos deben adaptarse en consecuencia. Por ejemplo, los fabricantes pueden necesitar cumplir con estándares seguros de desarrollo y parcheo, mientras que propietarios y operadores deben mantener prácticas seguras de configuración y monitorización. Establecer expectativas consistentes en la cadena

de suministro ayuda a reducir el riesgo sistémico y previene vulnerabilidades introducidas por productos o servicios de terceros.

## Seguro por diseño / Seguro por defecto

La adopción de principios de secure-by-design y secure-by-default ayuda a mitigar los riesgos de ciberseguridad antes de desplegar los sistemas. En lugar de depender únicamente de medidas defensivas tras descubrir vulnerabilidades, estos enfoques enfatizan la integración de la seguridad en tecnologías y procesos desde el principio. Esto incluye el diseño de sistemas con autenticación fuerte, servicios expuestos mínimos, configuraciones seguras y mecanismos de actualización robustos habilitados por defecto. Fomentar que fabricantes y operadores prioricen la seguridad durante el desarrollo y el despliegue reduce la probabilidad de debilidades explotables y fortalece la resiliencia a largo plazo de los sistemas de infraestructura crítica.

## Fortalecer la Respuesta y Recuperación Coordinada a Incidentes

La protección efectiva de infraestructuras críticas requiere capacidades sólidas y coordinadas de respuesta y recuperación a incidentes tanto en el sector público como en el privado. Los gobiernos y operadores deben establecer marcos claros para el intercambio de información, permitiendo el intercambio oportuno de inteligencia de amenazas, vulnerabilidades y datos de incidentes, respetando la confidencialidad y las restricciones legales.

Fortalecer los canales de comunicación de confianza entre operadores de infraestructuras, reguladores y autoridades de ciberseguridad puede mejorar significativamente la conciencia situacional y la eficacia de la respuesta.

Las pruebas regulares mediante ejercicios conjuntos, como simulaciones de incidentes cibernéticos que afectan a entornos de TI y OT, ayudan a garantizar que los roles, responsabilidades y procedimientos de respuesta estén bien comprendidos y sean operativos. Además, la planificación de la recuperación debe priorizarse junto con los esfuerzos de respuesta, incluyendo el desarrollo de estrategias de continuidad del negocio y restauración del sistema adaptadas a contextos de infraestructuras críticas. Dada la naturaleza interconectada de los sistemas digitales, los mecanismos de cooperación transfronteriza también son esenciales en América Latina para abordar amenazas transnacionales, coordinar respuestas y apoyar la rápida recuperación tras incidentes a gran escala.

## Invierte en una fuerza laboral más fuerte

La ciberseguridad para infraestructuras críticas en América Latina requiere una inversión sostenida en el desarrollo de la fuerza laboral, especialmente para profesionales que trabajan en la intersección de entornos de TI y OT. Muchos países de la región carecen de profesionales cualificados en ciberseguridad con experiencia especializada en sistemas de control industrial, lo que deja lagunas en la protección de servicios esenciales. Los gobiernos y los actores industriales

deberían priorizar el desarrollo de programas de educación y formación específicos centrados en la seguridad de las OT, incluyendo asociaciones con universidades, institutos técnicos y organismos internacionales de certificación.

Ampliar el acceso a certificaciones estandarizadas y formación práctica puede ayudar a construir una red de profesionales cualificados capaces de afrontar amenazas en evolución. Al cultivar una fuerza laboral de ciberseguridad altamente cualificada y estable, los países latinoamericanos pueden mejorar su capacidad para gestionar riesgos, responder a incidentes y mantener la resiliencia a largo plazo en los sectores de infraestructuras críticas.

# Conclusión

A medida que América Latina continúa modernizando su infraestructura y ampliando la conectividad digital, la seguridad de las infraestructuras críticas debe seguir siendo una prioridad central para gobiernos, operadores y socios industriales. La convergencia de los entornos de TI y OT, la creciente dependencia de servicios en la nube e inteligencia artificial, y la creciente complejidad de las cadenas de suministro globales han transformado fundamentalmente el panorama de riesgos para sectores críticos. Al mismo tiempo, el auge de la ciberactividad patrocinada por el Estado—especialmente desde China y Rusia—ha introducido un entorno de amenazas más estratégico y persistente, en el que los adversarios buscan no solo explotar vulnerabilidades, sino también preposicionarse dentro de sistemas críticos para posibles interrupciones durante crisis geopolíticas. Los resultados de la encuesta presentados en este documento destacan tanto el progreso alentador como las persistentes brechas, especialmente en las áreas de planificación de seguridad específica para OT, visibilidad de la cadena de suministro y preparación ante amenazas emergentes.

Las experiencias de otras jurisdicciones demuestran que la protección eficaz de infraestructuras críticas requiere estrategias coordinadas que combinen liderazgo político, marcos regulatorios, estándares del sector y colaboración público-privada. Las estrategias nacionales de ciberseguridad que abordan explícitamente la tecnología operativa, marcos dedicados a la seguridad OT, principios de seguridad de la cadena de suministro y regulaciones regionales armonizadas pueden contribuir a construir sistemas más resilientes. Al mismo tiempo, las organizaciones responsables de infraestructuras críticas deben fortalecer la gobernanza interna, mapear las intersecciones entre los entornos de TI y OT, y adoptar prácticas de seguridad por diseño que integren la seguridad a lo largo de todo el ciclo de vida tecnológico.

En última instancia, proteger infraestructuras críticas no es únicamente un desafío de ciberseguridad, sino un requisito estratégico para la estabilidad económica, la seguridad pública y la resiliencia nacional. La creciente prevalencia de campañas como Volt Typhoon y Salt Typhoon ilustra aún más que la infraestructura crítica es ahora un punto focal de la competencia estratégica a largo plazo, obligando a gobiernos y operadores a prepararse tanto para amenazas inmediatas como para riesgos latentes y preposicionados dentro de sus redes. Aprendiendo de las mejores prácticas globales e invirtiendo en una gobernanza más sólida, el desarrollo de la fuerza laboral y la cooperación intersectorial, los países latinoamericanos pueden reducir el riesgo sistémico y construir sistemas de infraestructura más seguros y fiables capaces de apoyar el crecimiento a largo plazo y la estabilidad regional.


DIGI
AMERICAS