2026

Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD

Resiliencia cibernética en las infraestructuras críticas de América Latina y el Caribe

ANÁLISIS DOCUMENTAL Y ESTRATÉGICO DE LA RESILIENCIA CIBERNÉTICA EN INFRAESTRUCTURAS CRÍTICAS

VIEM
Vicerrectoría de Innovación y Emprendimiento

ECBTI
Escuela de Ciencias Básicas, Tecnología e Ingeniería

Semillero de Investigación
Ceros y Unos

E-boletín Informativo CSIRT Académico UNAD

Medio de divulgación: Correo Electrónico, Sitio Web

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

Número treinta y ocho [38]
Abril de 2026

Universidad Nacional Abierta y a Distancia (UNAD)

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

Estado legal:
Periodicidad: Mensual
ISSN: 2806-0164

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

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

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

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

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

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

Centro de Desarrollo Tecnológico
CSIRT Académico UNAD
Ing. Luis Fernando Zambrano Hernández
Líder CSIRT Académico UNAD

Responsable de la Edición
Ing. Luis Fernando Zambrano Hernandez

Revisó
Ing. Nestor Raúl Cárdenas Corral
Analista CSIRT Académico UNAD

Contenido

Introducción

La transformación digital de los servicios esenciales ha incrementado la dependencia de las infraestructuras críticas frente a sistemas interconectados, plataformas digitales, redes de comunicación y proveedores tecnológicos. Sectores como salud, energía, telecomunicaciones, transporte, gobierno y servicios financieros requieren altos niveles de disponibilidad, integridad y continuidad operativa, debido a que una interrupción puede generar impactos sociales, económicos e institucionales significativos (Kure et al., 2022)

En este contexto, la resiliencia cibernética se convierte en una capacidad estratégica, ya que no se limita a prevenir ataques, sino que permite anticipar amenazas, proteger activos, detectar eventos, responder oportunamente, recuperar servicios y aprender de los incidentes. Marcos como el NIST Cybersecurity Framework 2.0 y la ISO/IEC 27001:2022 orientan la gestión del riesgo, la gobernanza de la seguridad y la mejora continua en las organizaciones (National Institute of Standards and Technology, 2024)

En América Latina y el Caribe, el fortalecimiento de la resiliencia cibernética continúa siendo un desafío, debido a brechas relacionadas con talento especializado, inversión, coordinación institucional, dependencia tecnológica y adopción parcial de estándares internacionales. Estas debilidades aumentan la exposición de las infraestructuras críticas frente a incidentes como ransomware, ataques a proveedores, interrupciones de servicios y afectaciones a la información sensible (Diaz & Nuñez, s. f.)

Por lo anterior, el presente documento analiza el estado de la resiliencia cibernética en las infraestructuras críticas de América Latina y el Caribe, identificando sus principales brechas, desafíos y buenas prácticas. El propósito es aportar una visión académica que permita comprender la importancia de integrar tecnología, gobernanza, gestión del riesgo, continuidad operativa, talento humano y cooperación interinstitucional para proteger los servicios esenciales (Banco Interamericano de Desarrollo & Organización de los Estados Americanos, s. f.)

Resiliencia cibernética, gobernanza y ciberseguridad institucional en infraestructuras críticas:

Retos estratégicos para un CSIRT académico en la protección de infraestructuras críticas

Autores

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

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

Yenny Stella Nuñez Alvarez
Docente Investigador
Universidad Nacional Abierta y a Distancia
ORCID: 0000-0002-6868-6278

Libardo Cárdenas Corral
Analista CSIRT Académico UNAD
Universidad Nacional Abierta y a Distancia
ORCID: 0000-0002-6868-6278

Estado actual de la resiliencia cibernética en las infraestructuras críticas de América Latina y el Caribe

La resiliencia cibernética se ha convertido en una capacidad estratégica para la protección de las infraestructuras críticas, especialmente en un escenario donde los servicios esenciales dependen cada vez más de plataformas digitales, redes de comunicación, sistemas de información, servicios en la nube, proveedores tecnológicos y entornos interconectados. Sectores como la salud, energía, transporte, telecomunicaciones, gobierno, servicios financieros y servicios públicos requieren altos niveles de disponibilidad y continuidad operativa, debido a que cualquier interrupción puede generar impactos institucionales, económicos, sociales y reputacionales.

En este marco, la ciberseguridad ya no se puede ver como un conjunto de controles técnicos encaminado a prevenir ataques; muy al contrario, debe ser considerada como una funcionalidad institucional que articula la gestión del riesgo, la continuidad de negocio, la conducta de la protección de la información, la respuesta a los incidentes, así como a la recuperación de los servicios que resulten afectados. (Kure et al., 2022) también argumentan que la gestión del riesgo en ciberseguridad debe abordarse con

una visión global, dado que la digitalización aumenta la superficie de exposición de las organizaciones y requiere de capacidades coordinadas para identificar las amenazas, evaluar las vulnerabilidades y mitigar los impactos. Esta postura reviste un interés importante para la discusión de las infraestructuras críticas, ya que la afectación de las mismas puede poner en peligro servicios esenciales para la sociedad.

La complejidad de infraestructuras críticas las define como los sistemas y activos, los procesos y los servicios cuyas disrupciones tienen consecuencias drásticas para la seguridad, la economía, la salud pública, la estabilidad institucional o el bienestar de la sociedad. Ya en Latinoamérica y el Caribe, las infraestructuras críticas están en buen camino hacia la transformación digital, lo que no obstante ha incrementado su exposición a amenazas como los ransomware, los phishing, las intrusiones no autorizadas, los asaltos a los sistemas industriales, la explotación de vulnerabilidades, las interrupciones de servicios digitales y la pérdida de confianza en los proveedores tecnológicos. La digitalización aumenta la eficiencia operativa, pero a cambio requiere esfuerzos crecientes de preparación, de monitoreo, de respuesta y recuperación.

La resiliencia cibernética permite expandir el enfoque tradicional de la seguridad preventiva. No se reduce solamente a impedir incidentes, sino a procurar que las organizaciones puedan anticipar amenazas, resistir eventos dañinos, responder de forma coordinada, recuperar operaciones y aprender de lo que ha ocurrido. En esa línea, (Küfeoğlu & Akgün, 2023) argumentan que la resiliencia cibernética debe perfilarse como un enfoque integrador, tendiente a desarrollar capacidades para seguir prestando servicios críticos aun en situaciones de incidentes de seguridad. Esto significa que garantizar la protección de las infraestructuras críticas no solo depende de las herramientas tecnológicas sino también de las políticas, de los procesos, del talento humano especializado, del liderazgo, de la cultura de la seguridad, como también de la cooperación.

Desde un punto de vista normativo, la ciberresiliencia se aborda según marcos de referencia tan reconocibles como la ISO/IEC 27001:2022 y el marco NIST en ciberseguridad, de forma que la norma ISO/IEC 27001:2022 muestra criterios para la implementación de un Sistema de Gestión de la Seguridad de la Información fundamentado en riesgos, controles, responsabilidades, auditorías y mejora continua (International Organization for Standardization (ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements, s. f.)), y el NIST las sistematiza en funciones como identificar, proteger, detectar, responder y recuperar, lo cual permite definir las acciones orientadas a la protección de los activos críticos y a la

continuidad de la operación (National Institute of Standards and Technology (National Institute of Standards and Technology, 2018); aunque el NIST 2018 no se refiere a la extensión de 2022 en adelante sigue siendo una referencia técnica muy reconocible para poder moldear el ciclo operativo respecto de la resiliencia.

En lo que concierne a la situación de la región de América Latina y el Caribe, en materia de ciberresiliencia se presentan hitos, pero a su vez brechas importantes. El documento base identifica, como problema regional, la existencia de capacidades desiguales, baja formalización de planes de respuesta y recuperación, escaso talento especializado disponible, adopción parcial de estándares internacionales, dependencia con proveedores tecnológicos y poca coordinación público-privada. Las brechas que hemos explicado evidencian que la región se encuentra en una construcción de capacidades, en donde hay políticas, lineamientos y marcos de referencia, pero su implementación es aún irregular.

La escasez de talento especializado es una de las fallas más relevantes. La resiliencia cibernética implica tener analistas de seguridad, personal de respuesta a incidentes, expertos en continuidad de negocio, gestores del riesgo, administradores de infraestructuras, expertos en ciberseguridad OT/ICS y responsables, responsables de gobernancia. Las organizaciones no cuentan con equipos profesionales para hacer frente a las capacidades avanzadas como SOC, SIEM, EDR/XDR, análisis de vulnerabilidades, gestión de incidentes, monitoreo continuo. Por lo tanto, ello influirá negativamente en la capacidad de detección temprana, contención, recuperación y aprendizaje para los eventos cibernéticos.

La apropiación de los marcos e referidos constituye otra de las fallas importantes, aunque en este caso son fallas relacionadas, dado que aunque existan marcos como ISO/IEC 27001:2022; NIST CSF; ENISA; NIS2, la apropiación de los mismos depende de la madurez institucional, presupuesto, liderazgo o capacidades técnicas adecuadas. Según el trabajo de gula líquida de la Comisión Económica para América Latina y el Caribe (Diaz & Nuñez, s.f.), los ciberataques a la infraestructura crítica en América Latina y el Caribe con un enfoque que busca dotar de capacidad institucional y autodefensa a sectores estratégicos, el problema no es solamente conocer los estándares sino convertirlos en controles y que estos sean evaluables y sostenibles.

La continuidad operativa es un componente fundamental de la resiliencia cibernética. Las organizaciones resilientes cuentan con planes de continuidad del negocio, planes de recuperación ante desastres, copias de seguridad verificadas, vías alternativas de operación, procedimientos de comunicación de crisis y simulaciones. (ENISA THREAT LANDSCAPE 2022, 2022)

advierte que el panorama de amenazas implica fortalecer la preparación institucional ante incidentes complejos, predominantemente en sectores donde la interrupción de servicios puede tener consecuencias severas. En el caso de las infraestructuras críticas, la preparación permite acortar tiempos de indisponibilidad, proteger información sensible y soportar la prestación de servicios esenciales. Asimismo, la resiliencia cibernética requiere de una perspectiva de gobernanza. Nos referimos a definir responsabilidades, políticas, priorizar activos críticos, gestionar proveedores, articular áreas internas, reportar incidentes y promover la mejora continua. La Directiva NIS2 de la Unión Europea no se aplica directamente en América Latina pero puede servir como referente comparativo porque refuerza obligaciones sobre gestión de riesgos, notificación de incidentes, continuidad operativa y responsabilidad institucional (Diaz & Nuñez, s. f.) En el caso latinoamericano, este tipo de orientaciones puede servir para nutrir regulaciones nacionales y marcos de protección de operadores esenciales.

Por lo tanto, la actual situación de la resiliencia cibernética en América Latina y el Caribe debe verlo como un proceso en curso. De hecho, los países de la región han progresado con el desarrollo de políticas públicas, la implementación de estrategias nacionales, la generación de equipos de respuesta y el reconocimiento de la relevancia que tiene el campo de la ciberseguridad. De todas formas, ante ello, existen todavía desafíos relacionados con el organismo de talento, las inversiones, la coordinación, la madurez tecnológica, la gestión de terceros y la formalización de planes de respuesta. Dichas condiciones corroboran la necesidad de que la resiliencia cibernética requiera de un enfoque integral donde la tecnología esté complementada por la gobernabilidad, la cultura de la seguridad, la cooperación y la gestión del riesgo.

Finalmente, la resiliencia cibernética de las infraestructuras críticas debe considerarse como una capacidad institucional orientada a proteger la continuidad de los servicios esenciales. Su afianzamiento implica que sean de una visión reactiva a un modelo preventivo, adaptativo y recuperativo, en definitiva, debe implicar la anticipación de amenazas, la protección de los activos críticos, la detección de los eventos, la respuesta oportuna, la recuperación de las operaciones y el aprendizaje de cada incidente. Desde esta perspectiva, América Latina y el Caribe deben afianzar capacidades sostenibles que tiendan a disminuir el impacto de los ciberataques y asegurar que los sectores salud, energético, telecomunicaciones, transporte, público y servicios financieros puedan mantener su operación frente a unas amenazas digitales cada vez más complejas.

Marcos normativos, políticas públicas y lineamientos internacionales sobre resiliencia cibernética en América Latina y el Caribe

La ciberresiliencia en las infraestructuras críticas no puede ser analizada únicamente bajo el punto de vista técnico, puesto que, por su fortaleza, también depende de marcos normativos, políticas públicas, normas internacionales, gobernanza institucional y mecanismos de coordinación de los actores públicos y privados. Una vez acotados los fundamentos conceptuales de la ciberresiliencia, es imprescindible revisar los referentes que orientan la práctica de su puesta en marcha en sectores críticos como: salud, energía, telecomunicaciones, transporte, el gobierno, servicios financieros y servicios públicos.

Los marcos normativos constituyen un referente estratégico en tanto organizan la gestión del riesgo, definen responsabilidades, protegen los activos críticos, establecen los controles de seguridad, dan respuesta ante incidentes y garantizan la continuidad. Así, la ciberresiliencia no es sólo una reacción ante los ataques sino una capacidad institucional para identificar los riesgos, prevenir afectaciones, detectar los eventos, responder de forma ágil y recuperar los servicios críticos.

Uno de los referentes más utilizados es el NIST CYBERSECURITY FRAMEWORK que estructura la gestión de la ciberseguridad en cinco funciones: identificar, proteger, detectar, responder y recuperar. Este modelo resulta relevante para las infraestructuras críticas porque permite evaluar el estado de madurez de una organización, priorizar activos esenciales y establecer acciones progresivas de mejora. Aunque su versión inicial fue publicada en 2018, sigue siendo un marco de referencia ampliamente utilizado para orientar la gestión del riesgo cibernético en organizaciones públicas y privadas (National Institute of Standards and Technology, 2018).

También es importante destacar que la norma ISO/IEC 27001:2022 constituye un referente significativo, dado que estamos ante una norma internacional que prescribe criterios para la implementación de un Sistema de Gestión de Seguridad de la Información. Su principal valor estriba en la formalización de políticas, controles, auditorías, gestión de riesgos, mejora continua y la efectiva asignación de responsabilidades. En el ámbito de las infraestructuras críticas, esta norma facilita la mejora de la gobernanza de la seguridad de la información, la mejora de la trazabilidad de los controles y la institucionalización de la cultura por la protección de la información y la continuidad de la operativa (ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements, s. f.)

Por otro lado, la Directiva NIS2 de la Unión Europea también puede constitutir un referente importante, a pesar de no ser de aplicación de forma inmediata en América Latina y el Caribe. Su aportación radica en que establece obligaciones para los operadores de servicios esenciales y las entidades críticas en aspectos como la gestión de riesgos, el reporte de incidentes, la continuidad del negocio, la supervisión regulatoria y la rendición de cuentas institucional. Para la región latinoamericana esta norma puede resultar útil como referencia comparativa para el fortalecimiento de regulaciones nacionales propias relacionadas con las infraestructuras críticas y los servicios digitales esenciales (NIS2 Directive: securing network and information systems, s. f.)

Instituciones como la Organización de los Estados Americanos, la Comisión Económica para América Latina y el Caribe y el Banco Interamericano de Desarrollo han elaborado estudios y, a partir de ellos, orientaciones que permiten comprender el estado de la ciberseguridad en la región. Los informes constituyen un claro avance en términos de estrategias nacionales, creación de equipos de respuesta a incidentes, fortalecimiento de capacidades y la significación del riesgo cibernético como tema estratégico. Sin embargo, también dan cuenta de las brechas en relación con el talento en ciberseguridad, la inversión, la coordinación interinstitucional, la madurez técnica y la efectividad en el nivel de adopción de estándares (Banco Interamericano de Desarrollo y Organización de los Estados Americanos, s. f.); Comisión Económica para América Latina y el Caribe (Diaz y Nuñez, s. f.); Organización de los Estados Americanos (Banco Interamericano de Desarrollo y Organización de los Estados Americanos, s. f.).

Según Diaz y Nuñez (s. f.), los ciberataques contra infraestructura crítica en América Latina y el Caribe revelan la necesidad de fortalecer las capacidades institucionales de prevención, respuesta y recuperación. Dicha perspectiva se considera transcendental para enlazar la ciberseguridad con la estabilidad de sectores estratégicos y con la continuidad de servicios que son esenciales para la ciudadanía, así como también los aportes de ENISA permiten entender que el panorama de amenazas considera que se tiene que tener mayor capacidad de preparación ante incidentes altamente complejos, sobre todo en entornos en donde la interrupción de servicios puede generar impactos de gran alcance (ENISA THREAT LANDSCAPE 2022, 2022).

En el caso colombiano, la Política Nacional de Seguridad Digital y los lineamientos propuestos desde el MinTIC y el de COLCERT representan un avance importante para el ejercicio de la gestión del riesgo digital, la protección de activos estratégicos y la coordinación entre, por ejemplo, las entidades públicas y las empresas del sector privado, sin embargo, el principal reto consiste en llevar a cabo

la transformación de estos lineamientos en acciones de producción medibles y sostenibles, sobre todo en sectores donde la interrupción de servicios digitales puede a su vez ocasionar la restricción de derechos, la ejecución de trámites, la oferta de servicios de salud, los procesos institucionales o la disponibilidad de información crítica.

En definitiva, las regulaciones, las políticas públicas y las normas internacionales son la base necesaria para avanzar en la resiliencia cibernética en América Latina y el Caribe. No obstante, esto sólo depende de la capacidad real de las instituciones para ponerlo en práctica, entendiendo que la aplicación de esas normas debe acompañarse de controles técnicos, de la capacitación del personal, de planes para la continuidad del negocio, del monitoreo continuo, la gestión de las incidencias, auditorías y la cooperación interinstitucional. Por ello, América Latina y el Caribe debe dejar de formular normas y pasar a hacer normas efectivas toda vez que se implementen a través de las capacidades requeridas para anticipar, proteger, detectar, responder y recuperar los servicios esenciales ante un ciberincidente.

Avances, brechas y desafíos de la resiliencia cibernética en infraestructuras críticas de América Latina y el Caribe

Los avances que ha dado América Latina y el Caribe son paulatinos, aunque su reconocimiento de la ciberseguridad como una cuestión estratégica para la protección de las infraestructuras críticas ha ido en ascenso. En los últimos años, una serie de países de la región han incrementado sus políticas nacionales de seguridad digital, han formado equipos de respuesta a incidentes, han concretado estrategias de gestión del riesgo y han empezado a firmar marcos internacionales centrados en la protección de sectores como el de la salud, la energía, las telecomunicaciones, el transporte, los servicios gubernamentales y los servicios financieros. Sin embargo, estos avances no han sido homogéneos, debido a diferencias en capacidades institucionales, presupuesto, talento especializado, madurez tecnológica y coordinación entre actores públicos y privados.

Uno de los mayores progresos en la región consiste en la integración de la ciberseguridad en las agendas de transformación digital. Según la Organización de los Estados Americanos y el Banco Interamericano de Desarrollo, la región ha incrementado sus esfuerzos en políticas públicas, cooperación internacional y desarrollo de capacidades nacionales en ciberseguridad, aun existiendo desequilibrios en cuanto a la gobernanza, así como en la aplicación e implementación (Banco Interamericano de Desarrollo & Organización de los Estados Americanos, s. f). Esto permite verificar como la resiliencia cibernética no sólo consiste en la existencia de marcos normativos sino de la transformación

de estos en capacidades reales de prevención, detección, respuesta y recuperación de bienes esenciales.

Pero aun existiendo estos avances, una de las brechas más importantes persiste en la escasez de talento especializado. La protección de las infraestructuras críticas requiere de líderes con competencias en materia de gestión del riesgo, monitoreo, respuesta a incidentes, continuidad de negocio, análisis de vulnerabilidades, seguridad de entornos industriales y recuperación de desastres. De acuerdo con el Foro Económico Mundial (2023), la insuficiencia de talento en ciberseguridad constituye una de las limitaciones globales más significativas para abordar las amenazas informáticas más complejas, una situación que afectará especialmente a las regiones donde las capacidades técnicas no se distribuyen igualmente. En la región de América Latina y el Caribe, esta brecha limita la explotación de capacidades como SOC, SIEM, EDR/XDR, análisis forense, inteligencia de amenazas y la gestión coordinada de incidentes.

Otra brecha importante corresponde a la adopción parcial de las normas internacionales. Aunque normas como la ISO/IEC 27001:2022 o el Marco de Ciberseguridad del NIST son ampliamente conocidas, su implementación requiere liderazgo institucional, recursos, procesos documentados, auditorías, responsables definidos y mejorar continuamente. Con frecuencia se conocen en organizaciones de la región como "estándares", pero no se confirman como controles verificables, planes de continuidad, simulaciones o como mecanismos de recuperación eficaces. La gestión del riesgo cibernético debe ser una gestión integrada que articule amenazas, vulnerabilidades, activos, impactos y controles, y debe serlo sobre todo en contextos donde la interrupción de la tecnología puede afectar a los servicios críticos (Kure et al., 2022).

Asimismo, persisten retos relacionados con la recuperación ante incidentes y la continuidad de la operativa. Un ataque a los servicios esenciales es capaz de comprometer la disponibilidad de las plataformas digitales, de la confidencialidad de la información, de la integridad de los datos, de la confianza de los usuarios (Diaz & Nuñez, s. f.) advirtiendo que en América Latina y el Caribe los ciberataques a la infraestructura crítica han puesto de manifiesto las carencias en la preparación institucional, especialmente en el caso de que las entidades no dispongan de planes formales para la respuesta, la recuperación y las de comunicación de crisis. Lo expuesto, asegura que la resiliencia cibernética debe ser considerada una capacidad organizacional y no únicamente una capacidad tecnológica.

La dependencia de los proveedores tecnológicos, se convierte en otro desafío relevante. Existen muchas instituciones que externalizan servicios críticos a los terceros, lo cual también

amplía la superficie de la exposición y que requiere controles contractuales, auditorías, acuerdos de niveles de servicio, la gestión de los accesos, la trazabilidad de los incidentes y la supervisión continuada. Según el (ENISA THREAT LANDSCAPE 2022, 2022) las cadenas de suministros y los proveedores tecnológicos constituyen vectores de riesgo relevantes, por lo que su gestión debe formar parte de cualquier plan de resiliencia cibernética.

Por todo lo anterior, América Latina y el Caribe han partido de logros políticos, conciencia institucional y marcos de referencia, pero la resiliencia cibernética se sigue construyendo. Las principales brechas están en la escasez de talento, fomento del cumplimiento de estándares, continuidad operativa y de terceros, coordinación interinstitucional y capacidades para detectar y responder a incidentes. Por lo anterior, el fortalecimiento regional tiene que pasar de diagnósticos generales a acciones concretas, medibles y sostenibles para proteger los servicios esenciales frente a la amenaza de ciberincidentes cada vez más complejos.

Las mejores prácticas, tecnología y los enfoques para la resiliencia cibernética en infraestructuras críticas

El fortalecimiento de la resiliencia cibernética en la infraestructura crítica exige un planteamiento global que articule tecnología, gobernanza, gestión del riesgo, talento humano, continuidad de la actividad y cooperación institucional. En los sectores de salud, energía, telecomunicaciones, transporte, gobierno, servicios financieros y servicios públicos, no basta con adoptar herramientas tecnológicas de ciberseguridad en forma aislada, hay que consolidar capacidades organizativas que sean capaces de anticipar, proteger, detectar, responder, recuperar y aprender frente a los incidentes que lleguen a tener lugar.

La primera práctica que merece la pena mencionar es la adopción de marcos de referencia internacionalmente reconocidos; efectivamente, el NIST Cybersecurity Framework 2.0 adopta el enfoque basado en funciones que se traduce en gobernar, identificar, proteger, detectar, responder y recuperar, permitiendo con ello que la gestión del riesgo cibernético se pudiera caracterizar como progresiva y adaptable a grados de organización y progresos madurativos distintos (National Institute of Standards and Technology, 2024). Este marco puede resultar el apropiado para la gestión de infraestructuras críticas al priorizar los activos, definir los controles, y elaborar las hojas de ruta para mejorar la postura de ciberseguridad.

Por su parte, la norma ISO/IEC 27001:2022 es, sin duda, la forma de poner en marcha un Sistema de Gestión de la Seguridad de la Información; la forma de encararla y

de tratar los riesgos ya permite el desarrollo de políticas, responsabilidades, controles, auditorías, procesos de mejora continua, etc. Todo lo que se debería dar para gestionar mejor la gobernanza de seguridad y proteger su confidencialidad, integridad y disponibilidad (ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements, s. f.)

Desde el componente tecnológico, las organizaciones que se ocupan de la infraestructura crítica deben optar por reforzar sus capacidades de monitoreo, deteeción y respuesta. Para ello, la recomendación es por implementar o bien reforzar soluciones como SOC, SIEM, EDR/XDR, IDS/IPS, WAF, inteligencia de amenazas o gestión de vulnerabilidades. Gracias a estas herramientas se puede mediante correlación de eventos, detectar el comportamiento anómalo, responder en el tiempo adecuado y reducir el tiempo de exposición a las amenazas. De forma explícita (Kure et al., 2022) manifiestan que la gestión de riesgo cibernético ha de incorporar activos, amenazas, vulnerabilidades, controles e impactos, contenidos que entran en la misma línea de pensamiento en que la estructura del proceso de gestión de riesgo de las amenazas cibernéticas ha de conjugar el elemento tecnológico y el elemento análisis de riesgo.

Otra de las estrategias básicas sería reforzar la continuidad operativa. Para las infraestructuras críticas es importante tener planes de continuidad del negocio, planes de recuperación ante desastres, copias de seguridad verificadas, respaldos inmutables, canales alternos de operación y ejercicios periódicos de simulación. (ENISA THREAT LANDSCAPE 2022, 2022) apuntan que el panorama de amenazas requiere preparar a las organizaciones en escenarios complejos, sobre todo aquellos en que la interrupción de los servicios puede afectar funciones críticas. La resiliencia no ha de medirse por la capacidad de evitar ataques, sino por la que reporta la posibilidad de sostener o recuperar los servicios en tiempos aceptables.

La dependencia de los proveedores de tecnología supone otro reto de interés. Pues en muchas entidades se encargan a terceros servicios críticos que incrementan la superficie de exposición a la vez que requieren controles contractuales, auditorías, acuerdos de nivel de servicio, gestión de accesos, trazabilidad de incidentes y supervisión continua. (ENISA THREAT LANDSCAPE 2022, 2022) advierte que las cadenas de suministro, al igual que los terceros proveedores de tecnología son vectores relevantes de riesgo, por lo que su gestión debe ser parte de cualquier estrategia de resiliencia cibernética propuesta.

En los entornos industriales y operacionales, como energía, agua, transporte o manufactura, es muy recomendable fortalecer la seguridad OT/ ICS mediante la segmentación de redes, el inventario de activos, los controles de acceso privilegiados, la

gestión de parches, el monitoreo especializado, el cifrado de comunicaciones y los procedimientos de recuperación operativa. Tales controles son de importancia porque en estos entornos un incidente no sólo podría afectar la información, sino que también podría afectar la prestación física de servicios que resultan ser esenciales.

Adicionalmente, la gestión de terceros también ha de ser vista como buena práctica prioritaria. La dependencia de los proveedores de tecnología requiere contratos en los que figuren las cláusulas de seguridad, los acuerdos de nivel de servicio, las auditorías técnicas, la trazabilidad de incidentes, los controles de acceso y la evaluación de riesgos de forma continuada. La Directiva NIS2 resalta la importancia de la gestión de riesgos, la notificación de incidentes y la responsabilidad de las entidades esenciales frente a sus cadenas de suministro y proveedores críticos (*DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022*, 2022).

la ciberseguridad en la organización. Las organizaciones deberán formar grupos especializados, capacitar usuarios, llevar a cabo simulaciones de phishing, reforzar los CSIRT/SOC, documentar las lecciones aprendidas, e impulsar la cooperación entre la administración pública, empresas privadas, academia y organismos de carácter especializado. De este modo, la resiliencia cibernética es un proceso que resulta ser gradual, medible y permanente cuyo objetivo es el de reducir el impacto de los incidentes y garantizar la continuidad de los servicios esenciales.

Ciclo de la resiliencia cibernética en infraestructuras críticas

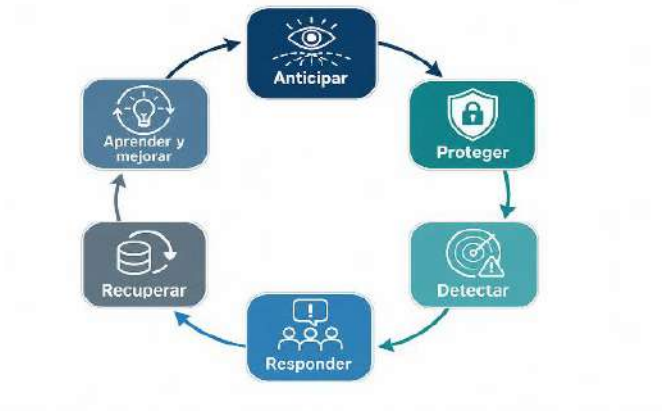
La resiliencia cibernética en infraestructuras críticas debe entenderse como un proceso continuo y no como una acción aislada de protección tecnológica. Su valor estratégico reside en que permite a las organizaciones adelantarse a las amenazas, proteger los activos esenciales, detectar eventos anómalos, responder de forma coordinada, recuperar operación y aprender de cada incidente en un proceso de fortalecimiento de la postura de seguridad. Este ciclo se relaciona con el enfoque del NIST Cybersecurity Framework 2.0, el cual incorpora funciones orientadas a gobernar, identificar, proteger, detectar, responder y recuperar frente al riesgo cibernético (National Institute of Standards and Technology, 2024).

En el contexto de las infraestructuras críticas, este ciclo será más relevante puesto que la interrupción por/r para sectores tales como Salud, Energía, Telecomunicaciones, Transporte, Gobierno o Servicios Financieros podría generar impactos de tipo social, económico, institucional de gran magnitud. Por eso, la resiliencia no ha de restringirse solamente a la prevención de ataques, sino también ha de integrar gestión del riesgo,

continuidad, respuesta a incidentes, recuperación de servicios y mejora. Dicho proceder coincide con la ISO/IEC 27001:2022, que plantea también la necesidad de gestionar la seguridad de la información mediante controles, responsabilidades, evaluación de riesgos y mejoras continuas (ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements, s. f.) y en la medida que el ciclo permite evidenciar que la resiliencia cibernética depende de la articulación de capacidades técnicas, talento humano, gobernanza y la cooperación institucional la anticipación y protección tienden a reducir la exposición; la detección y respuesta tienden a reducir el impacto, la recuperación y el aprendizaje tienden a robustecer a la organización frente a eventos futuros. En este sentido, (Kure et al., 2022) resaltan que la gestión del riesgo cibernético debe abordarse de forma integral, considerando activos, amenazas, vulnerabilidades, controles e impactos. De igual manera, (*ENISA THREAT LANDSCAPE 2022*, 2022) advierte que el panorama actual de amenazas exige capacidades más sólidas de preparación, monitoreo, respuesta y recuperación.

Figura 1

Ciclo de resiliencia cibernética en infraestructuras críticas: anticipar, proteger, detectar, responder, recuperar y aprender.



Nota. Elaboración propia con base en el enfoque de resiliencia cibernética asociado a la gestión del riesgo, la continuidad operativa y las funciones de protección, detección, respuesta y recuperación propuestas por (National Institute of Standards and Technology, 2024), (*ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*, s. f.), (Kure et al., 2022) *y* (*ENISA THREAT LANDSCAPE 2022*, 2022).

Conclusiones

La resiliencia cibernética de las infraestructuras críticas de América Latina y el Caribe debe considerarse como una capacidad estratégica y no sólo como una variable técnica de la ciberseguridad. Su importancia radica en que permite anticipar, proteger, detectar, responder, recuperar y aprender frente a incidentes que pueden afectar a servicios esenciales, tales como salud, energía, telecomunicaciones, transporte, gobierno, servicios financieros y servicios públicos.

La región ha logrado desarrollar políticas públicas, estrategias nacionales de ciberseguridad, adoptar marcos internacionales e, incluso, crear capacidades de respuesta a incidentes; si bien estas iniciativas continúan siendo desiguales entre países, sectores e instituciones, lo que da cuenta de que la resiliencia cibernética en América Latina y el Caribe continúa siendo un proceso en construcción que requiere mayor articulación, inversión y sostenibilidad.

Una de las brechas más críticas que se han documentado es la escasez de talento humano especializado en ciberseguridad, gestión del riesgo, continuidad operativa, respuesta a incidentes y protección de entornos críticos, que limita la capacidad de las organizaciones para explotar cada uno de los medios de las herramientas avanzadas, analizar amenazas, contener incidentes y recuperar servicios esenciales en los tiempos óptimos.

La adopción de marcos de referencia, tales como ISO/IEC 27001:2022. NIST Cybersecurity Framework, ENISA y NIS2, representa una oportunidad clara para fortalecer la gobernanza, la gestión del riesgo y la continuidad operativa. Sin embargo, esta mejora estará condicionada a que las organizaciones sean capaces de pasar de la norma marco a la implementación de controles, de procedimientos, de auditorías, de responsables configurados y de mejora continua de los mismos.

La protección de las infraestructuras críticas necesita adoptar una óptica integradora que relacione con toda la riqueza de la disciplina la tecnología con los procesos, las personas y la cooperación interinstitucional. Herramientas como SOC, SIEM, EDR/XDR, WAF, IDS/IPS, MFA, copias inmutables, segmentación, monitorización OT/ICS son esas herramientas que no deben faltar, pero son poco efectivas si no van acompañadas de un plan de continuidad, de gestión de vulnerabilidades, de cultura de la seguridad, de ejercicios de simulación y del liderazgo de la organización.

Finalmente, el desarrollo de la resiliencia cibernética de Latinoamérica y el Caribe tiene que dirigirse hacia acciones concretas, medibles y sostenibles, priorizando la protección de los servicios esenciales y la reducción del impacto de los incidentes. La región ha de transitar hacia modelos de ciberseguridad más maduros, coordinadores y ajustados a su realidad, en los que la continuidad operativa, la gestión del riesgo y la cooperación entre el Estado, el sector privado, la academia y los organismos especialistas deben formar parte del corpus teórico necesario para enfrentarse a las amenazas digitales cada vez más complejas.

CSIRT ACADÉMICO UNAD

Recomendaciones

Es conveniente hacer hincapié en que los países e instituciones de América Latina y el Caribe deben llevar a cabo la mejora de la resiliencia cibernética de las infraestructuras críticas apoyándose en una estrategia holística en la que intervenir la gobernanza, la gestión del riesgo, la continuidad operativa, el capital humano y las capacidades técnicas, en la que la protección de sectores como salud, energía, telecomunicaciones, transporte, gobierno o servicios financieros no dependa sólo de las tecnologías, sino de un modelo institucional que permita anticipar, detectar, responder y recuperarse a partir del ciberincidente.

Se debe recomendar la implementación de marcos como ISO/IEC 27001:2022, el NIST Cybersecurity Framework, el ENISA o NIS2 de manera gradual, medible y contextual para cada país, sector e institución para que no queden como referencias documentales, sino que se conviertan en controles reales, políticas aplicables, responsables definidos, auditorías periódicas, planes de mejora y procedimientos verificables en la protección de activos críticos.

Se recomienda, en paralelo, un fortalecimiento prioritario del talento humano especializado en ciberseguridad, gestión del riesgo, respuesta a incidentes, continuidad de negocio, seguridad OT/ICS y análisis de vulnerabilidades, de forma que sin personal capacitado, herramientas como SOC, SIEM, EDR/XDR, WAF o IDS/IPS no tienen valor, pues la resiliencia cibernética depende de la tecnología, pero también de la capacidad interpretativa de alertas así como del desarrollo de decisiones y de la coordinación de acciones.

Se instrumentará la recomendación para que las entidades responsables de las infraestructuras críticas formalicen y pongan a prueba periódicamente la vigencia de los planes de continuidad del negocio, de recuperación ante desastres y de respuesta a incidentes, que tienen que contemplar copias de seguridad verificadas e inmutables, sitios alternativos de operación, protocolos de comunicación de crisis, ejercicios de simulación, responsables por proceso y tiempos máximos de recuperación, al mismo tiempo que se asegura que la continuidad de los servicios esenciales llegue a mantenerse frente a los eventos cibernéticos.

Se instrumentará la recomendación para intensificar la cooperación interinstitucional entre estado, sector privado, academia, CSIRT/CERT nacionales, organismos internacionales y proveedores tecnológicos. La característica transnacional de las ciberamenazas demanda definir mecanismos de intercambio de información, alertas tempranas, ejercicios conjuntos y buenas prácticas compartidas junto a la coordinación operativa, en particular cuando los incidentes puedan comprometer servicios esenciales y provocar impactos de alcance social, económico o institucional.

Referentes

Banco Interamericano de Desarrollo, (BID), & Organización de los Estados Americanos, (OEA). (s. f.). *CIBERSEGURIDAD RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINA Y EL CARIBE*. Recuperado https://publications.iadb.org/es/publications/spanish/viewer/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Diaz, R. M., & Nuñez, G. (s. f.). *Ciberataques a la logística y la infraestructura crítica en América Latina y el Caribe*. Recuperado https://mexico.un.org/sites/default/files/2023-09/cepal.pdf

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022. (2022, diciembre 14). https://eur-lex.europa.eu/eli/dir/2022/2555/oj

ENISA THREAT LANDSCAPE 2022. (2022, octubre). https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202022.pdf

ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements. (s. f.). Recuperado https://www.iso.org/standard/27001

Küfeoğlu, S., & Akgün, A. T. (2023). *Cyber Resilience in Critical Infrastructure* (1.ª ed.). CRC Press. https://doi.org/10.1201/9781003449522

Kure, H. I., Islam, S., & Mouratidis, H. (2022). An integrated cyber security risk management framework and risk predication for the critical infrastructure

protection. *Neural Computing and Applications*, *34*(18), 15241-15271. https://doi.org/10.1007/s00521-022-06959-2

National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* (NIST CSWP 04162018; p. NIST CSWP 04162018). https://doi.org/10.6028/NIST.CSWP.04162018

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29; p. NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

NIS2 Directive: Securing network and information systems. (s. f.). Recuperado https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

Contactenos

📧 **Correo electrónico:** csirt@unad.edu.co
🌐 **Página web:** https://csirt.unad.edu.co

El CSIRT Académico UNAD está siempre disponible para apoyarte ante consultas o inquietudes relacionadas con la protección de la información en la universidad. No dudes en ponerte en contacto con nuestro equipo para recibir asesoría, reportar incidentes o recibir orientación en temas de seguridad digital. ¡Tu seguridad es nuestra prioridad!