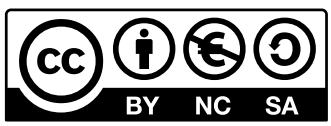
INTERCAMBIO
DE INFORMACIÓN
EN LATAM:

COMPRENDIENDO EL ROL DE LOS ISAC EN LA REGIÓN

DIGI AMERICAS



Para más información, por favor contacte con admin@digiamericas.org

Digi Americas Alliance

Alain Karioty
Alexis Steffaro
Andrea Escobedo
Andy Kotz
Belisario Contreras
Brett DeWitt
Carlos Torales
Christian Torres
Cory Bullock
Fernando Quintero
Gene Yoo
Ghassan Dreibi
Hernan Armbruster
Jordana Siegel
José Juan Haro
Mario de la Cruz Sarabia
Mauricio Benavides
Mauricio Nanne
Norberto (Bert) Milan
Patrick Ford
Rafael Alvarez
Ricardo Villadiego
Ryan Goss

Editores

Belisario Contreras
Alexis Steffaro
Pallavi Bhargava

DIGI AMERICAS ALLIANCE MEMBERS

aws Apple CHECK POINT CISCO CLOUDFLARE CROWDSTRIKE fluid attacks we hack your software Google
kriptos LUMU METABASE Q netskope paloalto NETWORKS Resecurity
Santander Schneider Electric Telefónica tenable Trellix TREND MICRO

Resumen

La rápida transformación digital de la región de América Latina y el Caribe (LATAM) ha aumentado significativamente su vulnerabilidad a los ciberataques, y el actual enfoque fragmentado del intercambio de información sobre ciberseguridad limita las capacidades de respuesta ante incidentes. Este documento explora el papel de los Centros de Análisis e Intercambio de Información (ISACs, por sus siglas en inglés,) como solución para mejorar la resiliencia regional. Proporciona una visión general de las estructuras de los ISAC, modelos de gobierno y los beneficios que ofrecen a los miembros, haciendo hincapié en su potencial para abordar los desafíos de ciberseguridad únicos de LATAM. Al examinar las iniciativas de intercambio de información existentes en la región, el documento pone de relieve las principales brechas, como los esfuerzos aislados en los sectores público y privado. El análisis destaca la necesidad de disponer de ISAC escalables, formalizados y adaptados a la dinámica operativa y cultural de LATAM. Si bien este documento no prescribe una estructura de ISAC específica, resalta la necesidad crítica de estos centros en la forma que mejor se adapte al contexto único de la región. Además de establecer ISAC formalizados, se recomienda aprovechar los esfuerzos de intercambio de información existentes e integrarse en las redes globales de ISAC cuando sea pertinente. Estos enfoques tienen como objetivo fomentar la participación de múltiples partes interesadas, reducir las brechas de desarrollo en ciberseguridad y capacitar a las partes interesadas regionales para implementar mecanismos de colaboración que mejoren la resiliencia y aborden las amenazas específicas de LATAM.

Tabla de Contenidos

Introducción

La región de América Latina y el Caribe (LATAM) ha aumentado rápidamente su dependencia de la infraestructura digital. Tras la pandemia de COVID-19, muchos servicios esenciales cotidianos, como la banca y la atención médica, se digitalizaron, haciéndolos cada vez más vulnerables a los ciberataques. Solo en Colombia, el 72% de todas las transacciones financieras se realizan a través de canales digitales.[1] Con la creciente dependencia digital, se necesitan estrategias digitales y protocolos de seguridad innovadores; los agentes privados de toda la región han expresado estas preocupaciones en sus llamados al cambio. El Centro México Digital reveló que "el 47% de las empresas latinoamericanas reconoce la necesidad de una estrategia digital y el papel esencial de la tecnología de la información en la continuidad comercial". Para 2023, el 72% de las empresas de la región habían comenzado a digitalizar sus operaciones, y México y Brasil se encontraban entre los 10 países con más usuarios de internet a nivel mundial.[2] Sin embargo, en 2021, solo tres países de América Latina habían diseñado una estrategia digital nacional, y aunque ese número ha crecido desde entonces, persiste una disparidad significativa entre el progreso del sector público y el privado.[3]

La dependencia digital de LATAM y la expansión del mercado de la ciberseguridad la han hecho altamente vulnerable a los ciberataques. Se estima que para 2025, LATAM podría experimentar un promedio de más de 18,5 millones de ataques por año, con costos anuales que superarían los 90 millones de dólares.[4] Los ataques de ransomware han sido los más comunes y perjudiciales, con países como Colombia, Brasil, Costa Rica, Chile, Panamá, entre otros, experimentando ataques de ransomware a gran escala y extremadamente perjudiciales en los últimos años.[5] El ransomware es un tipo de malware que impide a los usuarios acceder a sus dispositivos y a los datos almacenados en ellos, normalmente mediante el cifrado de archivos. Los delincuentes exigen entonces un rescate a cambio del descifrado. Solo Panamá experimentó un aumento del 421% en los ciberataques en los últimos dos años.[6] En 2023, el mercado de la ciberseguridad en América Latina estaba valorado en 8.340 millones de dólares. Además, se estimó que entre 2023 y 2028 el mercado global crecería a una tasa compuesta anual de alrededor del 6,95%, superando los 11.000 millones de dólares en 2028.[7]

---

[1] La Republica, Las transacciones digitales ya representan 72% dentro de las operaciones de los bancos, June 21, 2021, https://www.larepublica.co/finanzas/las-transacciones-digitales-ya-representan-72-dentro-de-las-operaciones-de-los-bancos-3187260#:~:text=Es%20decir%20m%C3%A1s%20de%2072,y%20con%20dat%C3%A1fonos%20692%20millones.
[2] BN Americas, Companies Embracing Change in Latin Americas Digital Transformation, January 24, 2024, https://www.bnamericas.com/en/news/companies-embracing-change-in-latin-americas-digital-transformation.
[3] Financial Services ISAC, Emerging Trends to Cyber Risks: a Latin American Perspective, https://www.fsisac.com/insights/emerging-trends-to-cyber-risks-latin-american-perspective, (last accessed July 26, 2024).
[4] Digi Americas, Cyber Readiness in Latin American Public Sectors, 2024, https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf.
[5] Ibid.
[6] Ibid.
[7] Statista, Value of the Cybersecurity Market in Latin America in 2023 and 2028, Jan. 2, 2024, https://www.statista.com/statistics/1180184/value-cybersecurity-market-latin-america/.

Existen importantes brechas de madurez cibernética en la resiliencia general de la ciberseguridad entre los países de LATAM, lo que lleva a una respuesta inconsistente ante incidentes en toda la región. Una "brecha de madurez cibernética" se refiere a la diferencia entre las capacidades actuales de ciberseguridad de una organización o país y el nivel de madurez que necesitan alcanzar, normalmente medido en comparación con un marco de ciberseguridad reconocido. Los países de LATAM se encuentran en diferentes etapas de desarrollo de políticas de ciberseguridad, lo que resulta en variaciones sustanciales en las tácticas de identificación y las prácticas de respuesta a incidentes de una nación a otra.

Se necesita un mecanismo cohesivo de intercambio de información en LATAM para generar resiliencia en la región.

Al compartir rápidamente información crítica sobre ciberataques y vulnerabilidades generalizadas, el alcance y la magnitud de los eventos cibernéticos pueden disminuir significativamente.[8] Dado que LATAM sigue siendo objetivo de amenazas maliciosas, la región necesita un foro cohesivo que reúna a todas las partes interesadas, tanto del sector público como del privado, para compartir información relevante sobre amenazas y mejores prácticas. Los Centros de Análisis e Intercambio de Información (ISAC, por sus siglas en inglés) prevalecen en EE.UU. y Europa y proporcionan un organismo central para recopilar y difundir información sobre amenazas cibernéticas a infraestructuras críticas dentro de un sector de infraestructuras críticas en concreto.[9] Tanto las partes interesadas del gobierno como los participantes del sector privado han identificado la necesidad de una iniciativa similar en LATAM, pero señalan que requerirá un enfoque único.

Los actuales esfuerzos de intercambio de información en LATAM están fragmentados, con los sectores público y privado operando en silos en lugar de en colaboración. Esta dinámica limita las oportunidades para el intercambio exhaustivo de información valiosa. Estos retos se ven agravados por los matices regionales, como la preocupación por parecer vulnerable al compartir información sobre amenazas, las preferencias culturales por los intercambios informales y la necesidad de abordar amenazas exclusivas de LATAM, como el malware específico de la región, como el troyano bancario Mekotio.[10] Este documento pretende explorar las consideraciones necesarias para la formación de ISAC en LATAM. En lugar de abogar por un modelo único, este documento hace hincapié en

[8] Cybersecurity and Infrastructure Security Agency (CISA), Information Sharing, https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing#:~:text=By%20rapidly%20sharing%20critical%20information,events%20can%20be%20greatly%20decreased. (Last accessed Sept. 27, 2024).
[9] National Council of ISACs, About ISACs, https://www.nationalisacs.org/about-isacs, (last accessed Jul. 19, 2024).
[10] Trend Micro, Mekotio Banking Trojan Threatens Financial Systems in Latin America, July 4, 2024, https://www.trendmicro.com/en_us/research/24/g/mekotio-banking-trojan.html.

la necesidad de iniciativas formalizadas y escalables para complementar y mejorar los enfoques puntuales existentes. Ya sean específicos de un sector o basados en un país, los ISAC en LATAM deben alinearse con la dinámica cultural y operativa de la región, aprovechando las prácticas existentes de intercambio de información y conectándose a las redes globales de ISAC cuando sea apropiado.

Este documento tiene como objetivo capacitar a las partes interesadas para decidir sobre la estructura ISAC que se ajuste a sus necesidades, destacando los beneficios, desafíos y fundamentos existentes para el intercambio de información en LATAM. Una mayor colaboración en la región puede ayudar a cerrar las brechas de madurez, mejorar la resiliencia, fomentar la confianza y abordar las amenazas de una manera que se adapte a las características únicas de la región.
El resto de este documento comienza con una introducción a los ISAC, incluyendo sus antecedentes, propósito, beneficios principales, desafíos, diferentes modelos estructurales, roles y responsabilidades, opciones de gobernanza y financiación, y capacidades clave. Posteriormente, se evalúa críticamente la necesidad de ISAC formalizados en LATAM, utilizando ejemplos específicos de la región para demostrar su alineación con las políticas emergentes y el deseo de una mayor colaboración entre múltiples partes interesadas. El documento continúa con una visión general de las iniciativas específicas de intercambio de información existentes en LATAM, identificando sus principales éxitos y puntos débiles. Por último, la conclusión ofrece la recomendación de que, independientemente de su estructura, la región LATAM se beneficiaría de mejores mecanismos formalizados de intercambio de información que aprovechen los esfuerzos existentes y superen el mero intercambio de información incorporando también iniciativas de educación y desarrollo de talento. Con estos cambios, sería posible trabajar para cerrar las amplias brechas de madurez en ciberseguridad que existen en la región.


50%
90%
100%

Componentes de un ISAC

Un ISAC, tal y como se define en EE.UU., es una organización sin fines de lucro, impulsada por sus miembros, que proporciona un recurso central para recopilar, analizar y difundir inteligencia sobre amenazas a sus miembros, al tiempo que permite un intercambio bidireccional de información entre los sectores público y privado. Los ISAC pueden adoptar diversas estructuras, que van desde modelos que incluyen únicamente a representantes de la industria del sector privado hasta otros que incorporan a participantes gubernamentales y de la sociedad civil. Aunque muchos de los ISAC existentes operan dentro del sector privado, este documento aboga por un enfoque multilateral basado en las prácticas actuales para mejorar la inclusión y la colaboración. Los ISAC crean un ecosistema de confianza entre sus miembros, lo que permite a los propietarios y operadores de infraestructuras críticas protegerse mejor a sí mismos y a sus clientes de las amenazas cibernéticas y físicas. Además de reuniones anuales, intercambios técnicos, talleres y seminarios en línea, los ISAC ofrecen servicios de alerta de amenazas y notificación de incidentes las 24 horas del día. Los ISAC son un tipo de asociación público-privada (PPP, por sus siglas en inglés), pero se consideran un mecanismo más formal que las PPP tradicionales, ya que sus miembros siguen un marco claramente definido para compartir información y análisis. Mientras que la mayoría de los ISAC de EE.UU. y la Unión Europea siguen un enfoque sectorial, la siguiente sección explora los diferentes modelos estructurales para construir un ISAC que será pertinente que la comunidad de LATAM considere cuando comience a formalizar el intercambio de información en la región.

HISTORIA Y ADOPCIÓN INTERNACIONAL

El concepto de los ISAC se introdujo y promulgó por primera vez en virtud de la Directiva de Decisión Presidencial-63 (PDD-63) de EE.UU., firmada el 22 de mayo de 1998, tras la cual el gobierno federal pidió a cada sector de infraestructuras críticas que estableciera organizaciones sectoriales específicas para compartir información sobre amenazas y vulnerabilidades.[11] Entre los ISAC estadounidenses más destacados figuran el ISAC de Servicios Financieros (FS ISAC), el ISAC de Salud (H-ISAC), el ISAC de Tecnologías de la Información (IT-ISAC) y el ISAC Multiestatal (MS-ISAC), entre muchos otros.[12] Los ISAC sectoriales colaboran entre sí a través del Consejo Nacional de ISAC (NCI, por sus siglas en inglés), un organismo de coordinación diseñado para maximizar el intercambio de información entre las infraestructuras críticas del sector privado y con el gobierno. [13] El NCI proporciona un foro para compartir amenazas y estrategias de mitigación entre los ISAC y con socios gubernamentales y del sector privado durante incidentes que requieran una respuesta intersectorial. A través de una cadencia regular de reuniones, el NCI se coordina entre los centros de operaciones ISAC y realiza sus propios ejercicios y actividades según

[11] National Council of ISACs, About ISACs.
[12] National Council of ISACs, Member ISACs, https://www.nationalisacs.org/members, (last accessed Jul. 19, 2024).
[13] Ibid.

sea necesario.[14] La división de los ISAC por sectores de infraestructuras críticas permite a la plataforma mantener un conocimiento específico de la situación de todo el sector y tener en cuenta las realidades únicas de cada uno. Mientras que la mayoría de los ISAC de EE.UU. se centran en entidades con sede en ese país, los más maduros, como el FS-ISAC, cuentan con empresas miembros ubicadas a escala internacional y en LATAM.[15] Por ejemplo, las grandes empresas multinacionales suelen ser miembros de ISAC estadounidenses y pueden ser miembros de más de uno en función de su ámbito de interés.

A medida que los ISAC han ido creciendo en número y madurez en los Estados Unidos, también se han adoptado en la Unión Europea (UE) de muchas formas diferentes. En la UE, los ISAC existen en estructuras formales e informales y pueden estar centrados en un país, en un sector o ser internacionales. Los primeros ISAC de la UE se centraron en los sectores financiero y energético. El enfoque de la UE respecto a los ISAC es único en el sentido de que a menudo se espera apoyo gubernamental, principalmente para facilitar funciones, además de ofrecer experiencia y conocimientos profesionales como socio de un ISAC.[16] Además, la legislación europea apoya la creación de ISAC. En particular, la Directiva NIS 2 separa a los operadores de servicios esenciales en sectores y encarga a los operadores la aplicación de los requisitos sobre notificación de incidentes.[17] La creación de ISAC sectoriales a nivel nacional podría respaldar la aplicación de estas disposiciones al ser el punto de encuentro para la interacción entre las partes interesadas de los sectores público y privado.[18] A medida que la región LATAM continúa desarrollando la legislación sobre ciberseguridad, los gobiernos deben considerar cómo pueden incluir disposiciones que apoyen la creación de mecanismos de intercambio de información de manera similar a la Unión Europea.

Sin embargo, es importante señalar que este enfoque ha creado controversia debido a que muchos ISAC con sede en EE.UU. ya tienen una presencia significativa en la UE, lo que ha ocasionado confusión y la necesidad de conciliar funciones y responsabilidades que se superponen. LATAM debería tener en cuenta esta complejidad a medida que la región continúa desarrollando legislación e iniciativas en materia de ciberseguridad. Los gobiernos y las partes interesadas en LATAM pueden beneficiarse de la identificación proactiva de oportunidades para asociarse con las comunidades globales de intercambio de información existentes para minimizar la fragmentación, aprovechar la experiencia establecida y abordar las limitaciones presupuestarias. Estas asociaciones pueden reducir la necesidad de crear nuevos sistemas desde cero, garantizando soluciones rentables que se basen en modelos probados. Al considerar estos factores, LATAM puede diseñar mecanismos de intercambio de información que equilibren la necesidad de relevancia regional con las oportunidades de cooperación internacional, aprendiendo tanto de los éxitos como de los retos de la experiencia de la Unión Europea.

---

[14] National Council of ISACs, About NCI, https://www.nationalisacs.org/about-nci (last accessed Oct. 9, 2024).
[15] Financial Services ISAC, Emerging Trends to Cyber Risks: A Latin American Perspective.
[16] ENISA, ISACs Cooperative Models.
[17] The NIS 2 Directive, https://www.nis-2-directive.com/ (last accessed Oct. 22, 2024).
18 Ibid.

BENEFICIOS PRINCIPALES

Mejor postura de seguridad y defensa colectiva

El principal beneficio de un ISAC es proporcionar una defensa colectiva. Si una organización sufre un ciberataque, es muy probable que otras organizaciones de la región, o incluso del mundo, también lo sufran. Compartir información, mejores prácticas o medidas de corrección de ataques anteriores puede ayudar a los miembros del ISAC a ajustar sus defensas en consecuencia. Esto también anima a los miembros a tomar medidas proactivas contra las vulnerabilidades que se comparten dentro de un ISAC, evitando que esperen a que ocurra una catástrofe.[19]

Experiencia en ciberseguridad basada en la comunidad

Las entidades más pequeñas a menudo carecen de los recursos necesarios para supervisar constantemente las amenazas, evaluar los impactos y desarrollar planes de mitigación sólidos. Los recursos, la financiación y el personal para las iniciativas de ciberseguridad son frecuentemente difíciles de obtener, por lo que la participación en un ISAC permite a las organizaciones aprovechar la experiencia común de las entidades asociadas. Los miembros de un ISAC participan en seminarios web y talleres educativos y están en canales de comunicación y chats de grupo seguros que facilitan un acceso rápido y fiable a la información. Si una organización miembro de un ISAC tiene una pregunta específica de su sector, los canales de comunicación del ISAC le permiten preguntar a una red fiable de sus homólogos en lugar de recurrir a una investigación que cuesta tiempo. Los ISAC también tienen un historial de responder y compartir información procesable y relevante más rápidamente que los socios gubernamentales.[20]

Mayor confianza y resiliencia de la comunidad

Los ISAC fomentan una mayor confianza y un sentimiento de comunidad entre sus miembros, creando un entorno en el que se da prioridad a la colaboración y el apoyo mutuo. Esta confianza es crucial para abordar las amenazas cibernéticas en constante evolución, ya que fomenta el intercambio proactivo y oportuno de inteligencia procesable. Más allá del intercambio de inteligencia, los ISAC permiten a sus miembros alcanzar colectivamente una postura de seguridad sólida mediante la puesta en común de recursos y conocimientos, elementos que a menudo son inaccesibles para las organizaciones individuales por sí solas. Al aprovechar esta

[19] Health Sector Coordinating Council Cybersecurity Working Group, Health Industry Cybersecurity - Information Sharing Best Practices, Aug. 2023, https://healthsectorcouncil.org/wp-content/uploads/2023/08/HIC-ISBP-2023.pdf.
[20] National Council of ISACs, About ISACs.

conexión compartida, los ISAC mejoran la seguridad de la información y la resistencia ante las amenazas cibernéticas, al tiempo que minimizan los costos adicionales para sus miembros. [21] Por otra parte, los ISAC desempeñan un papel vital en la promoción de la alfabetización digital y el fomento de la comunicación, la colaboración y la capacidad de resolución de problemas entre sus miembros, principios clave alineados con el marco de alfabetización digital de la UNESCO. [22] Este sentido de comunidad, unido a las ventajas prácticas, hace que los ISAC tengan un valor incalculable en un panorama digital cada vez más interconectado.

Mejora de la innovación en ciberseguridad

Al aumentar el conocimiento de la situación en todo el sector mediante el intercambio de información, las organizaciones recibirán alertas avanzadas de amenazas y podrán tomar medidas proactivas para mitigar posibles intrusiones. A medida que continúan las innovaciones en los ataques, especialmente con la integración de la IA generativa que mejora las capacidades de los atacantes, los equipos de seguridad deben asegurarse de que sus organizaciones evolucionan junto con los desafíos únicos del sector, las normas y las mejores prácticas para mantener sus operaciones seguras. La colaboración con socios sectoriales a través de los ISAC permitirá a las entidades hacerlo.

Beneficios gubernamentales

La estrecha cooperación con los miembros del sector privado permite a las entidades públicas gubernamentales obtener una comprensión más profunda de los retos específicos de la industria, lo cual es muy valioso a la hora de dar forma a la legislación y la estrategia de ciberseguridad. Al participar en los ISAC, las entidades públicas pueden obtener información sobre la postura de ciberseguridad de sectores clave a través de información compartida sobre amenazas, incidentes y vulnerabilidades. Esta participación, cuando se aborda con respeto a los diferentes niveles de tolerancia para compartir información con el gobierno, puede ayudar a las entidades públicas a comprender mejor la evolución del panorama cibernético y mejorar su capacidad para apoyar a los sectores críticos. Además, esta colaboración ayuda a agilizar la comunicación y la coordinación, garantizando que las políticas y estrategias estén bien informadas y más alineadas con las necesidades prácticas de los sectores que pretenden proteger.

---

[21] Health Sector Coordinating Council Cybersecurity Working Group, Health Industry Cybersecurity - Information Sharing Best Practices, Aug. 2023, https://healthsectorcouncil.org/wp-content/uploads/2023/08/HIC-ISBP-2023.pdf.
[22] The World Bank, Digital Economy for Latin America and the Caribbean Country Diagnostic: Jamaica, pg. 118, April 2024, https://thedocs.worldbank.org/en/doc/61714f214ed04bcd6e9623ad0e215897-0400012021/related/IDU1c6883bf81f279148581a6dd184a5f721a2ea.pdf.

DESAFÍOS DEL ISAC

Aunque participar en un ISAC puede generar muchos beneficios tanto para los participantes como para el ecosistema de ciberseguridad en general, existen diversos desafíos que pueden suponer obstáculos para el éxito del intercambio de información.

Falta de recursos/financiación

El mayor desafío global para los miembros del sector público y privado de los ISAC es la falta de recursos humanos y financieros dedicados al intercambio y análisis de información. Se trata de un problema general del ecosistema de la ciberseguridad, pero se agrava en el análisis de la información. En concreto, afecta a las organizaciones que no tienen personal suficiente para dedicarse a participar activamente en el ISAC, así como a los gobiernos que tal vez no cuenten con la capacidad para desempeñar un papel administrativo o de facilitador. Esta falta de financiación y de personal dedicado puede suponer una barrera de entrada para las entidades más pequeñas y medianas. Es probable que las empresas más grandes y maduras tengan los medios para permitirse la membresía, lo que podría desviar la concentración de miembros de las entidades más pequeñas que más se beneficiarían de la afiliación. Además, debido a la amplia gama de niveles de madurez de los miembros y a los conocimientos cibernéticos preexistentes, la información compartida en el ISAC puede no ser comprendida por algunos miembros. Es tarea del ISAC contextualizar los recursos compartidos para que sean comprensibles por todos los participantes del grupo, independientemente de su dimensión y madurez. Muchos ISAC invierten las cuotas de sus miembros en programas de formación y capacitación para brindar acceso a niveles superiores de conocimientos técnicos.[23] Sin embargo, la falta de financiación puede afectar al nivel de análisis ofrecido a los participantes.

Nivel mínimo de experiencia/participación

Debido a los distintos niveles de madurez, los participantes de los ISAC deben tener un nivel mínimo de conocimientos técnicos y organizativos para participar activamente en las actividades de intercambio de información y ejercicios. Un esquema de colaboración exitoso debe estructurarse con incentivos para el intercambio activo de información, de modo que todos los miembros participen activamente. También es fundamental implicar a los ejecutivos de nivel C, además del personal técnico, en los ejercicios de intercambio de información y formación. De este modo, se demuestra el valor de un ISAC a los líderes ejecutivos y se pueden asignar fondos empresariales específicos a dichos recursos.

[23] Ibid.

Creación de confianza/diferencias culturales

La preocupación por la privacidad y la confidencialidad está siempre presente entre los posibles miembros de un ISAC, pero los ISAC existentes aplican importantes medidas de protección de la privacidad de los datos. Estas medidas suelen incluir estrictos controles de acceso, técnicas de anonimato y canales de comunicación seguros.[24] Los ISAC también consultan con expertos legales para diseñar planes que garanticen el cumplimiento de las normativas de privacidad, y los ISAC consultan con expertos políticos externos para mantenerse actualizados sobre los cambios en las leyes y regulaciones.[25] Los ISAC son conscientes de la necesidad de encontrar el equilibrio entre un intercambio de información abierto y productivo y la preocupación por la privacidad. Otras preocupaciones comunes pueden ser las barreras lingüísticas, las diferencias culturales o los distintos niveles de experiencia en diversos campos. Los ISAC pueden ofrecer servicios de traducción y tienden a normalizar los formatos y protocolos de intercambio de información para que el proceso sea lo más accesible posible en todos los sectores.[26] Por consiguiente, compartir información en un ISAC es una de las únicas maneras de comunicarse entre sectores con una base obligatoria de privacidad y seguridad. La idea de compartir abiertamente información para prevenir a los actores de amenazas puede parecer contraintuitiva, pero los ISAC son entornos en los que la confidencialidad y el intercambio ético son directrices rutinarias, y todos los miembros reciben el mismo trato.

Responsabilidades y roles transparentes

La flexibilidad inherente a los distintos modelos de estructura, gobernanza, roles y responsabilidades de un ISAC puede suponer un reto importante para las organizaciones que deseen establecer o participar en este tipo de iniciativas. Aunque esta flexibilidad permite una personalización basada en las necesidades específicas de la industria y los contextos regionales, también puede dar lugar a incoherencias en la forma de compartir y gestionar la información. La diversidad de marcos de gobernanza puede generar confusión en cuanto a los procesos de toma de decisiones y la rendición de cuentas, lo que dificulta que los miembros comprendan sus roles y responsabilidades. Además, los diferentes niveles de compromiso y asignación de recursos entre los miembros pueden crear una participación desigual, lo que podría obstaculizar la eficacia del ISAC. Esta falta de normalización puede complicar la colaboración y reducir la confianza general necesaria para el éxito del intercambio de información. Estos desafíos se agravan aún más en regiones como América Latina, donde existen disparidades significativas en la madurez organizativa con respecto a la comprensión y

[24] Blue Goat Cyber, The Impact of Information Sharing Analysis Centers on Cybersecurity, https://bluegoatcyber.com/blog/the-impact-of-information-sharing-and-analysis-centers-on-cybersecurity/, (last accessed July 26, 2024).
[25] Ibid.
[26] Ibid.

preparación de la ciberseguridad. No obstante, estos obstáculos pueden mitigarse adoptando un enfoque mixto que aproveche los modelos basados en los países y se centre al mismo tiempo en los sectores clave con mayores niveles de madurez, como el sector financiero. Esta alineación estratégica permite soluciones personalizadas que fomentan la colaboración, mejoran la confianza y, en última instancia, refuerzan la postura general de la región en materia de ciberseguridad.

MODELOS ESTRUCTURALES

Aunque existen muchos enfoques para organizar un ISAC, se han consolidado dos modelos principales:

- Modelo centrado en el país y
- Modelo sectorial.

Modelo centrado en el país

Este modelo de cooperación se centra en un único país, uniendo a todos los expertos y equipos de respuesta a incidentes de seguridad informática (CSIRT, por sus siglas en inglés) pertinentes bajo una única iniciativa. El modelo centrado en un país puede dar lugar a acuerdos informales regidos por la propia comunidad de CSIRT o a compromisos más formalizados gestionados por el gobierno de un país. Los ISAC facilitados por el gobierno son característicos de los países más pequeños, donde es más fácil para el sector público facilitar un ISAC debido al menor número de partes interesadas. Vea a continuación ejemplos de ISAC centrados en el país:

» **CERT.LU** – Iniciativa nacional para todos los equipos de respuesta a emergencias informáticas (CERT) de Luxemburgo, creada para intercambiar información entre la red de CSIRT del país.[27] Este ISAC está gobernado por la propia comunidad CERT.[28]

» **Finlandia** – El Centro Nacional de Ciberseguridad (NCSC-FI) gestiona varios ISAC. El NCSC-FI recopila y analiza información sobre amenazas a la seguridad procedente de diversas fuentes, como los ISAC y los sistemas de detección y alerta temprana, y luego comparte esa información con los componentes del NCSC-FI a través de múltiples canales, incluidos los ISAC.[29]

[27] The terms CSIRT (Computer Security Incident Response Team) and CERT (Computer Emergency Response Team) are often used interchangeably, but there are subtle differences in their origins and branding.
[28] CERT.LU, About CERT.LU, https://www.cert.lu/ (last accessed Oct. 18, 2024).
[29] ENISA, Information Sharing and Analysis Centres (ISACs) Cooperative Models, 2017, https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models?v2=1.

Modelo sectorial

Este modelo se centra en el nivel sectorial de las infraestructuras críticas con el objetivo de compartir información y análisis con otros expertos activos en el sector. Por lo general, este enfoque está liderado por actores del sector privado con una financiación mínima por parte del gobierno, especialmente en EE.UU., donde la financiación pública de los ISAC es poco común. Sin embargo, no existen restricciones a la financiación gubernamental, y los gobiernos de LATAM podrían proporcionar apoyo financiero caso por caso, especialmente en escenarios como el intercambio de información sobre incidentes específicos. El modelo sectorial se utiliza ampliamente en países más grandes que tienen un sector privado fuerte, con objetivos de ciberseguridad claramente definidos y mayores presupuestos asignados a los esfuerzos de intercambio de información. Vea a continuación ejemplos de ISAC sectoriales:

» **Servicios financieros (FS-ISAC)** – Fundado en 1999 para avanzar en la resiliencia de la ciberseguridad en el sistema financiero mundial mediante la protección de las instituciones financieras y las personas a las que sirven. Aunque el FS-ISAC tiene su sede en EE.UU., actualmente cuenta con miembros en más de 75 países, lo que demuestra la flexibilidad y el alcance que puede tener un único ISAC.[30]

» **El Centro de Ciberseguridad Bancaria (BCC) de Polonia** – Una plataforma para que los bancos se comuniquen e intercambien información sobre vulnerabilidades y amenazas relevantes. La afiliación está abierta a cualquier banco comercial de Polonia.[31] El BCC es un ejemplo de ISAC sectorial y centrado en el país.

Los ISAC sectoriales también pueden estructurarse para contar con participación internacional, ampliando el alcance del ISAC más allá de un único país. Los ISAC internacionales se enfrentan a desafíos a la hora de generar confianza, lo que puede resultar más difícil debido a las diferencias culturales de las partes interesadas.[32] Vea a continuación algunos ejemplos:

» **EU FI-ISAC** – El ISAC de las instituciones financieras europeas se creó en 2008 para intercambiar información sobre la actividad cibercriminal que afecta a la comunidad financiera europea. Sus miembros son representantes del sector financiero de cada país, CERT nacionales y fuerzas de seguridad. Otras organizaciones representadas son ENISA, Europol, el Banco Central Europeo (BCE), el Consejo Europeo de Pagos (EPC) y la Comisión Europea. El EUFI-ISAC cuenta con el apoyo activo de ENISA.[33]

---

[30] FS-ISAC, What We Do, https://www.fsisac.com/ (last accessed Oct. 18, 2024).
[31] ENISA, ISACs Cooperative Models.
[32] ENISA, ISACs Cooperative Models.
[33] ENISA, European Financial Institutes – Information Sharing and Analysis Centre, A Public-Private Partnership, https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/finance/european-fi-isac-a-public-private-partnership (last accessed Oct. 18, 2024).

» **EE-ISAC** – El objetivo del ISAC de energía europea es mejorar la resistencia y la seguridad de la infraestructura energética europea compartiendo información basada en la confianza y posibilitando un esfuerzo conjunto de análisis de amenazas. Entre sus miembros figuran proveedores técnicos y de servicios, empresas de servicios públicos, universidades, institutos de investigación y organizaciones gubernamentales y sin fines de lucro.[34]

ROLES Y RESPONSABILIDADES

Un ISAC es un mecanismo eficaz para facilitar la cooperación entre los sectores público y privado, pero es importante definir claramente los rolees y responsabilidades de todas las entidades implicadas para que la organización pueda funcionar de manera efectiva. En todo ISAC habrá un "facilitador", los "miembros" y los "socios" del ISAC. El facilitador desempeña el rol secretarial de establecer la logística del grupo, como definir la frencuencia de las reuniones, reclutar nuevos miembros y realizar actividades de marketing.[35] La mayoría de los facilitadores también proporcionan la infraestructura técnica y de procesos necesaria para permitir el intercambio de información, que va desde herramientas sencillas, como listas de correo electrónico, hasta plataformas sofisticadas para compartir y analizar indicadores de compromiso (IOC). Un miembro es una entidad que comparte y recibe activamente información como beneficio de la afiliación y que paga activamente las cuotas de afiliación para participar. Por último, los socios del ISAC incluyen expertos en la materia y entidades que participan en sesiones dedicadas, normalmente para ofrecer conocimientos específicos sobre un tema concreto. A continuación, se exploran las actividades de cada parte interesada relevante en un ISAC. Es importante señalar que la falta de claridad en los roles y responsabilidades impide el correcto funcionamiento de un ISAC.

Sector público

Las instituciones gubernamentales del sector público pueden desempeñar diferentes roles en un ISAC dependiendo de las circunstancias. Una administración puede cumplir con el rol de facilitador proporcionando lugares para las reuniones, además de otras funciones de secretaría. Los gobiernos pueden incluso asignar financiación directa para contribuir al desarrollo del ISAC. Alternativamente, las administraciones públicas pueden crear un marco legal tanto para el intercambio de información como para la creación de un ISAC.[36] Sin embargo, el papel de la administración pública varía en función del cometido de la entidad. Por ejemplo, las Agencias Nacionales de Ciberseguridad (NCA, por sus siglas en inglés) son organizaciones que suelen participar en los ISAC, ya sea facilitando el propio ISAC o participando activamente en el

[34] European Energy Information Sharing & Analysis Centre, Home, https://www.ee-isac.eu/ (last accessed Oct. 18, 2024).
[35] ENISA, ISACs Cooperative Models.
[36] ENISA, ISACs Cooperative Models.

intercambio y análisis de información. La mayoría de las NCA gestionan un CSIRT, que también es un organismo fundamental para participar en un ISAC. Es habitual que en torno a uno o dos organismos públicos participen en un ISAC, ya sea de forma regular o de manera puntual.

Fuerzas del orden y comunidad de inteligencia

Las fuerzas del orden y los servicios de inteligencia pueden ser socios valiosos en los ISAC por sus misiones especializadas y su acceso a información valiosa. En EE.UU., las fuerzas del orden y los ISAC colaboran de forma habitual, ya que gran parte de la información compartida por los organismos de seguridad no está clasificada en el sentido tradicional, aunque no esté a disposición del público. Sin embargo, los organismos de la comunidad de inteligencia (IC) suelen limitar su compromiso con los ISAC debido a la naturaleza clasificada de su información. No obstante, es importante mantener los vínculos con estas comunidades e incorporarlas como socios en sesiones temáticas específicas.

Industria y propietarios y operadores de infraestructuras críticas

La industria debe ser la principal impulsora de todos los ISAC, como facilitador y como miembro. Incluso cuando participa la administración pública, es la industria la que debe determinar la forma y la funcionalidad de su cooperación.[37] El sector privado es propietario de la mayoría de las infraestructuras críticas. A medida que la tecnología de las infraestructuras críticas y la prestación de servicios se vuelven más eficientes gracias a la transformación digital, los propietarios/operadores de activos dependen cada vez más del funcionamiento seguro y sin problemas tanto de la tecnología de la información (TI) como de la tecnología operativa (TO). Esto hace que la ciberseguridad sea un imperativo empresarial necesario para garantizar la prestación segura de servicios, la confianza pública y la continuidad de las actividades. Además, la participación de las empresas del sector debe abarcar una amplia gama de entidades, incluidos los propietarios/operadores de activos de infraestructuras críticas y los proveedores de tecnología operativa de cuyos productos tecnológicos dependen dichos propietarios/operadores.

[37] Ibid.

Mundo académico

Los ISAC suelen presentar al mundo académico como socio para que el gobierno y la industria puedan comunicar claramente sus necesidades en materia de investigación y desarrollo.[38] La interacción con el mundo académico puede dar lugar a nuevas soluciones para los sectores críticos y el panorama cibernético en general. También es un foro eficaz para que los investigadores comprueben la viabilidad o los resultados de su investigación en la práctica, al mismo tiempo que reciben comentarios de los propietarios y operadores de infraestructuras críticas.

GOBERNANZA Y FINANCIACIÓN

En consonancia con su naturaleza flexible, los ISAC pueden gobernarse de muchas maneras. Algunos tienen una estructura de gobernanza clara con roles bien definidos, como la secretaría y una junta directiva, mientras que otros no tienen una estructura clara y son comunidades flexibles en las que los voluntarios organizan las reuniones. Las principales actividades del ISAC (reuniones, ejercicios, etc.) están definidas por la estructura de gobernanza. Cuanto más estructurado esté un ISAC, más específicas serán las tareas a realizar. Sin embargo, con menos estructura, un ISAC puede ser menos activo y centrarse en casos especiales puntuales. Ambos modelos de gobernanza son válidos y pueden ajustarse a las necesidades de los miembros del ISAC.

Enfoque de gobernanza estructurada

La estructura de gestión de un ISAC puede variar. Algunos son dirigidos por un presidente y un vicepresidente, mientras que otros optan por una junta directiva o un comité directivo. Estos roles de liderazgo no suelen ser elegidos y pueden incluir una combinación de trabajo remunerado y voluntario, dependiendo del tamaño y el alcance del propio ISAC. Estos puestos suelen asignarse a miembros del sector privado o a organizaciones muy comprometidas con el ISAC. Una vez establecidos, su rol principal es desarrollar un plan estratégico que guíe los objetivos de la comunidad. Estas estructuras suelen incluir normas de elección y mandatos bien definidos.[39]

[38] ENISA, ISACs Cooperative Models.
[39] Ibid.

Gobernanza con un organismo de apoyo

En otros casos, un ISAC puede designar a una única entidad para que desempeñe el rol de secretaría. Esto es lo más habitual cuando el sector público participa en un ISAC. En este escenario, la administración pública supervisa las frecuentes interacciones del grupo para que se correspondan con una agenda detallada.

Gobernanza flexible

Algunos ISAC no tienen una estructura de gobernanza clara ni roles definidos, lo que da lugar a una comunidad muy flexible, normalmente dirigida por voluntarios. Una organización o representante diferente se ofrece voluntario para organizar cada reunión, rotando la responsabilidad cada vez. Estos ISAC no suelen tener un plan de acción formal, y las decisiones se toman sobre una base puntual para abordar los retos a medida que van surgiendo. Con este planteamiento flexible, las reuniones se celebran en distintos lugares, lo que permite a la comunidad conocer mejor las culturas de sus homólogos. Sin embargo, la falta de formalidad puede dar lugar a una menor participación de las partes interesadas.

Financiación

Al igual que la estructura y la gobernanza, existen múltiples maneras de financiar un ISAC, lo que será importante que LATAM tenga en cuenta cuando empiece a formalizar el intercambio de información en la región.[40]

- **Cuotas obligatorias** – Este es el modelo de financiación más común para un ISAC. Las cuotas se pagan anualmente y varían en función del tamaño y la participación de la entidad.
- **Contribuciones voluntarias** – En este modelo, los miembros proporcionan ayuda monetaria además de los recursos necesarios, como la organización de lugares de reunión, la asignación de personal dedicado a las actividades del ISAC, el desarrollo de grupos de trabajo, etc.
- **Subsidios gubernamentales** – Aunque es poco frecuente, los gobiernos pueden aportar financiación cuando existe un programa o un marco jurídico. Esta financiación suele cubrir la facilitación, como la gestión de una secretaría o la provisión de espacios para reuniones, y su objetivo es fomentar la participación de la industria más que sostener el ISAC a largo plazo.

[40] ENISA, ISACs Cooperative Models.

CAPACIDADES CLAVE

En esta sección se destacan las capacidades clave que un ISAC puede ofrecer a sus miembros:

Intercambio de información – El intercambio de información es la función central de un ISAC, permitiendo a los miembros intercambiar inteligencia crítica que les ayude a defenderse colectivamente contra las amenazas cibernéticas. Esto incluye indicadores de amenazas (como direcciones IP o firmas de malware); detalles de incidentes (como técnicas de ataque, intención e impacto); vulnerabilidades (en software, hardware o procesos de negocio); y estrategias de mitigación (como parches de seguridad o actualizaciones de antivirus). Los miembros también comparten mejores prácticas, desde estrategias de respuesta a incidentes hasta controles de seguridad. La información se comparte a través de plataformas seguras, incluidos portales web anónimos como MISP, correos electrónicos cifrados y reuniones presenciales. Al facilitar el intercambio oportuno y seguro de esta información, los ISAC permiten a las organizaciones adaptarse rápidamente a las amenazas emergentes, mejorando su resiliencia general y reduciendo la posibilidad de que se produzcan incidentes cibernéticos a gran escala.

Reuniones regulares y grupos de trabajo – Las reuniones regulares y los grupos de trabajo sobre temas específicos son esenciales para mantener la comunicación y fomentar la colaboración entre los miembros del ISAC. Estas reuniones unen a expertos y socios del sector para abordar cuestiones urgentes de ciberseguridad. Al proporcionar una plataforma para el diálogo continuo y el intercambio de conocimientos, los ISAC permiten una experiencia más profunda y una resolución de problemas más proactiva, garantizando que los miembros estén preparados para hacer frente a los riesgos cibernéticos en evolución.

Conferencias y eventos paralelos – Las conferencias y eventos paralelos dan a conocer las actividades del ISAC y amplían la participación de las partes interesadas. Estos actos permiten a los participantes conocer las tendencias emergentes, los avances tecnológicos y las estrategias de ciberseguridad. Los eventos paralelos, que pueden incluir talleres, mesas redondas y sesiones de capacitación, sirven como plataformas específicas para abordar áreas de interés o retos concretos dentro del sector. También ofrecen oportunidades para la creación de redes y la colaboración, aumentando la influencia y el alcance del ISAC dentro del sector. Estas reuniones son cruciales para mantener informadas y conectadas a las partes interesadas.

Ejercicios – Los ISAC realizan ejercicios para evaluar y mejorar la preparación de sus miembros en materia de ciberseguridad. Estos ejercicios pueden variar desde simulacros a nivel de gobernanza, que garantizan que los ejecutivos están preparados para tomar decisiones críticas, hasta simulacros operativos y técnicos que ponen a prueba la capacidad de una organización

para aplicar procedimientos y utilizar herramientas de ciberseguridad con eficacia.[41] Estos ejercicios son vitales para identificar brechas, validar la preparación y mejorar la capacidad de respuesta ante incidentes en todos los niveles de la organización.

Análisis – El análisis es un servicio clave de valor agregado proporcionado por los ISAC, que ayuda a los miembros a comprender y priorizar los riesgos cibernéticos. Los ISAC realizan **análisis de vulnerabilidades y amenazas** poniendo en común la experiencia de las organizaciones participantes, a menudo a través de grupos de trabajo conjuntos. Este enfoque colaborativo permite el desarrollo de una visión completa de las amenazas emergentes, ayudando a los miembros a anticipar y mitigar los riesgos. Aunque la realización de análisis detallados puede requerir muchos recursos, los miembros reconocen su valor y suelen estar dispuestos a asumir los costos.

Además, los ISAC ofrecen conocimientos jurídicos y reglamentarios vitales relacionados con el intercambio de información. Comprender el panorama legal es fundamental, ya que las leyes de privacidad y las obligaciones reglamentarias, como la notificación obligatoria de incidentes, pueden tanto plantear obstáculos como crear nuevas exigencias para el intercambio eficaz de información. Los ISAC ofrecen orientación sobre cómo compartir información sin dejar de cumplir estas normativas, ofreciendo a los miembros tranquilidad y fomentando intercambios de datos más abiertos.

Para los ISAC que carecen de un equipo de análisis especializado, la tarea de proporcionar un análisis coherente de las amenazas puede resultar abrumadora, ya que los grandes volúmenes de datos requieren tiempo y recursos considerables. En tales casos, la colaboración con agencias gubernamentales (por ejemplo, ENISA en iniciativas paneuropeas) puede ayudar a mejorar la capacidad analítica de los ISAC.[42]

Creación de confianza – La confianza es la base de cualquier ISAC eficaz. Al facilitar la interacción frecuente, los ISAC fomentan la comunicación abierta y la colaboración entre sus miembros. La creación de relaciones personales y el establecimiento de mecanismos formales, como acuerdos de confidencialidad, códigos de conducta, el uso de las normas de Chatham House y el Protocolo del Semáforo (TLP, por sus siglas en inglés), garantizan que los miembros se sientan seguros a la hora de compartir información sensible. La confianza mejora la efectividad general del intercambio de información, haciendo que un ISAC sea más resiliente y fiable.

---

[41] ENISA, Cross-Sector Exercise Requirements, March 2022, file:///C:/Users/acs07/Downloads/Cross-sector%20exercise%20requirements%20(1).pdf.
[42] ENISA, ISACs Cooperative Models.

Evaluación de la necesidad de un ISAC en LATAM

América Latina es una región altamente atacada por amenazas cibernéticas, impulsada por características regionales únicas que actúan como "aceleradores", tales como el uso generalizado de software sin licencia; altas tasas de piratería de software; y la rápida digitalización de sus mercados financieros, incluyendo el surgimiento de numerosas Empresas de tecnología financiera.[43] Las grandes brechas de madurez en la respuesta a incidentes y las capacidades de ciberseguridad que existen entre los países de LATAM los convierten en un objetivo principal para los actores de amenazas, con algunos países experimentando más de 1.000 ciberataques por segundo.[44] El valor total del mercado de la ciberseguridad en América Latina en 2024 fue de 8.920 millones de dólares, y se espera que esa cifra aumente hasta superar los 12.480 millones de dólares en 2029.[45] Las crecientes amenazas cibernéticas en LATAM presentan una necesidad significativa de mejorar el intercambio formal de información en la región. Esta sección revisa cómo la creación de ISAC en LATAM beneficiaría el panorama de amenazas y se alinearía con los objetivos políticos declarados relacionados con la gobernanza digital, la colaboración de múltiples partes interesadas y el desarrollo de la fuerza laboral.

La creación de ISAC en LATAM beneficiaría el panorama de amenazas y se alinearía con los objetivos políticos declarados relacionados con la gobernanza digital, la colaboración de múltiples partes interesadas y el desarrollo de la fuerza laboral.

PANORAMA DE AMENAZAS

La región de LATAM está altamente integrada: los ciberataques pueden afectar a entidades mucho más allá del alcance original de un ataque, lo que hace que la resiliencia regional sea crucial. Algunos países de LATAM ya están empezando a imitar los esfuerzos proactivos de los demás. Por ejemplo, tras la serie de ataques de ransomware en Costa Rica en 2023, El Salvador tomó medidas para desarrollar un sólido programa de ciberseguridad y actualizar sus políticas posteriores para evitar una situación similar.[46] Un ISAC proporcionaría un método formalizado para compartir las lecciones aprendidas y facilitar el desarrollo de políticas nacionales de ciberseguridad más sólidas en toda LATAM.

---

[43] Americas Quarterly, How Latin America's Governments Compare on Anti-Piracy, January 17, 2019, https://www.americasquarterly.org/article/how-latin-americas-governments-compare-on-anti-piracy/.
[44] Jamaica Major Organized Crime and Corruption Agency, Combatting Cyber Crime, https://www.moca.gov.jm/cyber-crime, (last accessed Jul. 25, 2024).
[45] Mordor Intelligence, Latin America Cybersecurity Market Size (2024-2029), https://www.mordorintelligence.com/industry-reports/latin-america-cyber-security-market/market-size, (last accessed Jul. 25, 2024).
[46] Telecommunications Industry Association, Costa Rica Takes Bold and Decisive Stance on Cybersecurity, Sept. 6, 2023, https://tiaonline.org/press-release/costa-rica-takes-bold-and-decisive-stance-on-cybersecurity/.

En la actualidad, LATAM depende de los países que participan activamente en el intercambio de información para la asistencia en la respuesta a incidentes, la financiación y la dirección en el desarrollo de estrategias cibernéticas. Cuando se producen incidentes cibernéticos, los países que participan en redes formalizadas de intercambio de información están mejor posicionados para responder y recuperarse de los ataques. Por ejemplo, Estados Unidos cuenta con la red de ISAC más sólida del mundo y ocupa el primer puesto en el índice cibernético mundial, con una puntuación de 100.[47] Cuando Costa Rica sufrió un ataque de ransomware que le costó el equivalente a 30 millones de dólares al día, Estados Unidos, Israel y España intervinieron. Estos países participan en ISAC cibernéticos y estaban equipados para ayudar en la situación de Costa Rica, en parte debido a los recursos y conocimientos que obtuvieron gracias a su mayor intercambio de información.[48] Por lo tanto, empezar a invertir en la creación de ISAC en LATAM mejorará la resiliencia regional y reducirá la dependencia de la región de socios externos.

No compartir información puede ser más peligroso que los riesgos que se corren al compartirla, porque muchos hackers ahora operan compartiendo sus propias estrategias entre sí para obtener mayor provecho.[49] Por ello, participar en un ISAC nivela el campo de juego contra los actores maliciosos que ya comparten su propia información. Así como la creación de confianza es un reto, también es una oportunidad para una mayor unidad regional. Los participantes en un ISAC pueden alertar proactivamente a sus homólogos de las amenazas más frecuentes y aprender de las experiencias compartidas por otros. Aunque la creación de confianza es un proceso a largo plazo, el éxito de los ISAC en otras partes del mundo demuestra el potencial positivo de los ISAC para mejorar la resiliencia cibernética regional.

ALINEACIÓN DE POLÍTICAS

El desarrollo de ISAC en LATAM se alinea con la creciente atención de la región a la gobernanza digital. Varios países han comenzado a desarrollar Estrategias Nacionales de Ciberseguridad o a proponer legislación para una Agencia Nacional de Seguridad Digital, que incluye el intercambio de información y una mayor colaboración de múltiples partes interesadas como iniciativas declaradas. Por ejemplo, Chile implementó una nueva política nacional de ciberseguridad en marzo de 2024, "Ley Chilena de Ciberseguridad e Infraestructura Crítica de la Información".[50] Como ley pionera en LATAM, su objetivo es promover la gestión de riesgos; implementar estándares de seguridad para mejorar la prevención,

[47] ITU Publication, Global Cybersecurity Index.
[48] Cytek Security, Enhancing the National Security Posture of Costa Rica with an Integrated Approach, Jan. 9, 2024, https://cytek-security.com/resources/enhancing-the-national-security-posture-in-costa-rica-with-an-integrated-approach/.
[49] Computer Security Online, What is an ISAC or ISAO?, July 26, 2022, https://www.csoonline.com/article/567485/what-is-an-isac-or-isao-how-these-cyber-threat-information-sharing-organizations-improve-security.html.
[50] National Cybersecurity Coordination, Chilean Government Enacts Cybersecurity Law, Mar. 26, 2024, https://ciberseguridad.gob.cl/en/news/chile-enacts-cybersecurity-law-creates-cybersecurity-agency/#:~:text=The%20digital%20security%20of%20Chileans,cybersecurity%20actions%20of%20State%20agencies.

incluyendo respuestas a ciberataques a través de asociaciones público-privadas (PPP, por sus siglas en inglés); y establecer obligaciones de ciberseguridad que resulten en sanciones si no se cumplen. La ley crea además un CSIRT Nacional y un Consejo Multisectorial, por lo que todas las organizaciones, públicas o privadas, entran en el ámbito del CSIRT si prestan servicios que afectan a infraestructuras críticas. Un ISAC, por definición, es el intercambio de información entre entidades públicas y privadas, el uso de la participación de múltiples partes interesadas, y el intercambio de amenazas y respuesta a incidentes de ciberseguridad relacionados con infraestructuras críticas. Estos tres aspectos fueron establecidos como objetivos en la Ley chilena, pero se implementaron de maneras diferentes y descentralizadas. El establecimiento de un ISAC consolidaría directamente a los objetivos chilenos existentes y unificaría su aplicación, facilitando el seguimiento de los avances.[51]

México participó en los esfuerzos para aumentar la coordinación y el intercambio de información cuando, en agosto de 2022, México y EE.UU. establecieron un "Grupo de Trabajo sobre Temas Cibernéticos" para promover un "compromiso compartido con un Internet abierto, interoperable, seguro y fiable y un ciberespacio estable".[52] Una iniciativa destacada del grupo de trabajo fue el fortalecimiento de los mecanismos de coordinación técnica para abordar las amenazas cibernéticas. Este es el objetivo central de un ISAC, lo que demuestra cómo un ISAC en LATAM se alinearía a la perfección con los esfuerzos ya en marcha en toda la región. Además, expertos de la industria en Brasil pidieron recientemente la creación de una Agencia Nacional de Seguridad Digital para centralizar los recursos y permitir la aplicación de la Estrategia Nacional de Ciberseguridad de Brasil. La agencia mantendría la ciberseguridad entre las principales prioridades del gobierno brasileño, algo crucial considerando que Brasil es el segundo país más vulnerable a los ciberataques a nivel mundial.[53]

Es importante señalar que las políticas varían mucho en su desarrollo, lo que crea brechas significativas en la preparación cibernética en toda LATAM. Según el GCI (Índice de Ciberseguridad Global de la UIT), México obtuvo una puntuación de preparación en ciberseguridad de 81,75, mientras que Honduras obtuvo una puntuación de 2,2.[54] La variabilidad en la preparación de la ciberseguridad es sustancialmente mayor en LATAM en comparación con otras regiones del mundo, lo que indica que la mejora del intercambio de información podría dar

[51] Lexology, Stepping up in Latin America: Chile enacts a new Cybersecurity Law, https://www.lexology.com/library/detail.aspx?g=82a52636-a23c-4b8b-9158-3203f69a3fb0#:~:text=Chile%20has%20also%20approved%20its,legislation%20and%20regulation%20in%20Chile, (last accessed July 25, 2024).
[52] Carnegie Endowment for International Peace, Mexico's National Cybersecurity Policy: Progress Has Stalled Under AMLO, May 28, 2024, https://carnegieendowment.org/research/2024/05/mexicos-national-cybersecurity-policy-progress-has-stalled-under-amlo?lang=en¢er=russia-eurasia.
[53] Center for Cybersecurity Policy and Law, Hearing Highlights Industry Calls for Brazilian National Digital Security Agency, July 16, 2024, https://www.centerforcybersecuritypolicy.org/insights-and-research/hearing-highlights-industry-calls-for-brazilian-national-digital-security-agency.
[54] ITU Publications, Global Cybersecurity Index 2020, https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E (last accessed July 24, 2024).

resultados significativos para los países de LATAM que se quedan atrás en la preparación cibernética.[55] Un ISAC puede cerrar esta brecha de madurez entre los países de LATAM compartiendo las lecciones aprendidas y animando a los actores más pequeños a tomar medidas proactivas para asegurar sus sistemas.

COLABORACIÓN MULTILATERAL

Los ISAC se alinean claramente con las iniciativas mundiales existentes de intercambio de información y colaboración público-privada. A partir de 2022, 99 países han firmado o ratificado un acuerdo multilateral sobre intercambio de información, y más de 140 países han participado en actividades internacionales, como conferencias sobre ciberseguridad, talleres, asociaciones y convenios con otros países.[56] Además, 86 países han participado en asociaciones público-privadas internacionales o nacionales, mientras que 62 países de todo el mundo han participado en ambas.[57] El intercambio de información ha demostrado su valor a nivel internacional, y los gobiernos de todo el mundo se han comprometido a aumentar su participación en asociaciones público-privadas y mecanismos de intercambio de información. Por ejemplo, un análisis de la economía digital de Jamaica realizado por el Foro del Banco Mundial concluyó que la falta de intercambio de información con el sector privado contribuía a debilitar la arquitectura de ciberseguridad del país. La investigación señaló que la "ausencia de foros formales y canales de comunicación para la cooperación con el fin de fomentar la confianza digital, y el limitado conocimiento compartido" limitan la resiliencia cibernética de Jamaica.[58] Por lo tanto, un ISAC en LATAM se alinea con el movimiento global hacia un mayor intercambio de información y podría aumentar la resiliencia de los países menos preparados cibernéticamente de LATAM.

Los actuales esfuerzos de intercambio de información en LATAM (que se analizan con más detalle a continuación) no se considerarían mecanismos formales como un ISAC, ya que no involucran a todo el espectro de partes interesadas relevantes y a menudo limitan la participación a otros homólogos gubernamentales a nivel nacional. Además, no existe una única plataforma centralizada para conectar las diversas iniciativas mencionadas anteriormente. La Red de CSIRT de las Américas de la OEA ejemplifica este problema, ya que la participación se limita a otros CSIRT gubernamentales, pero no incluye a las partes interesadas del sector privado o del mundo académico.[59] Otro ejemplo es el Foro de Equipos de Seguridad y Respuesta a Incidentes (FIRST), que pretende unir a los equipos de seguridad y respuesta a incidentes de la región y se basa en un modelo de gobernanza en red entre iguales de los

[55] ITU Publications, Global Cybersecurity Index.
[56] ITU Publications, Global Cybersecurity Index.
[57] ITU Publications, Global Cybersecurity Index.
[58] The World Bank, Digital Economy for Latin America and the Caribbean Country Diagnostic: Jamaica, pg. 153, April 2024, https://thedocs.worldbank.org/en/doc/61714f214ed04bcd6e9623ad0e215897-0400012021/related/IDU1c6883bf81f279148581a6dd184a5f721a2ea.pdf.
[59] CSIRT Americas, https://csirtamericas.org/en (last accessed July 24, 2024).

CSIRT.[60] Los avances en la creación de CSIRT nacionales son extremadamente positivos y han producido una cantidad significativa de inteligencia cibernética entre muchos proveedores. Sin embargo, o bien esta información no es visible para la mayoría de las organizaciones porque están excluidas de los actuales esfuerzos de intercambio de información, o bien las organizaciones carecen de la madurez y los mecanismos para procesar y comprender la información sobre amenazas que se ha recopilado.

Limitar la participación en los esfuerzos de intercambio de información solo restringirá aún más la capacidad de LATAM para combatir los crecientes ciberataques. Como región, cuando se producen incidentes, es crucial que todos los sectores tengan acceso a la información pertinente. Un ISAC en LATAM cubriría este vacío de información e involucraría a las partes interesadas de la industria privada y el mundo académico para que participen en el intercambio de información sobre amenazas y mejores prácticas, creando un entorno cohesivo en el que se incluya a todas las partes relevantes. Los ISAC también permiten a los actores menos maduros, como las pequeñas y medianas entidades, comprender y aplicar la información compartida. Sin un eje centralizado para el intercambio de información, muchos de los recursos en los que los países de LATAM están invirtiendo grandes sumas de tiempo y dinero podrían no utilizarse plenamente, ya que la participación es limitada. Un ISAC dedicado a LATAM también permitiría que la información compartida tuviera un verdadero contexto de LATAM en lugar de depender de socios internacionales sin la misma visión de los problemas regionales para fortalecer la ciberseguridad.[61]

ATRACCIÓN DE TALENTOS Y OPORTUNIDADES EDUCATIVAS

Los beneficios del intercambio de información van más allá de la respuesta a incidentes: un ISAC en LATAM podría ser un paso importante para aumentar la atracción y retención de talento cibernético, además de fomentar una comunidad más consciente de la ciberseguridad. LATAM experimenta grandes disparidades en el acceso a Internet en toda la región, lo que afecta a la viabilidad de la creación de una fuerza laboral cibernética. Si bien ha habido algunos avances en la creación de iniciativas educativas en ciberseguridad, estas son fragmentadas y la mayoría de los esfuerzos se realizan en áreas específicas. Aunque más de 1.600 universidades de la región ofrecen programas de grado y posgrado en formación en tecnologías digitales, se limitan a determinados países: Argentina, Brasil, Chile, Colombia, México, Perú, Ecuador, Costa Rica y Uruguay.[62] Además, dentro de estos países, Argentina alberga el 66% de las universidades que ofrecen dichos cursos.

---

[60] FIRST, Vision and Mission Statement, https://www.first.org/about/mission (last accessed Jul. 26, 2024).
[61] Trade EC Europa, Cybersecurity Sector in Central America, November 2022, https://trade.ec.europa.eu/access-to-markets/en/country-assets/euca_05_Cybersecurity%20sector%20in%20Central%20America.pdf.
[62] CEPAL, Latin American Economic Outlook 2020: Digital transformation for building back better, September 9, 2020, pg. 105.

Educar al público de LATAM en general sobre iniciativas, oportunidades y competencias básicas cibernéticas tiene el potencial de crear oportunidades laborales para el ~60% de los trabajadores de la región cuyo empleo es informal.[63] Sin embargo, esto requerirá que un mayor porcentaje de la población esté conectada digitalmente y educada para aumentar la fuerza laboral cibernética. En una encuesta de la CEPAL de 2020, el 75% de las zonas más ricas de América Latina y el Caribe utilizaban Internet, mientras que solo el 37% de la quinta parte más pobre tenía acceso a Internet.[64] Varios países de la región han empezado a ofrecer capacitación gratuita en línea sobre competencias digitales, como el Plan de Desarrollo de Competencias Digitales "IFT teaches you", los Centros de Transformación Digital Empresarial de Colombia y los Infocentros Comunitarios de Ecuador. En Brasil, la Red Nacional de Investigación y Educación (RNP), SENAI-SP y Softex crearon un curso gratuito de ciberseguridad llamado "Hackers do Bem" para los interesados en trabajar en el campo de la ciberseguridad.[65] Sin embargo, estos esfuerzos son puntuales y LATAM carece de recursos regionales globales para mejorar la alfabetización digital.[66] Para lograr un cambio significativo en la región, las oportunidades educativas deben tener un alcance más amplio, mejorando la comprensión colectiva en toda LATAM. Como centro neurálgico para académicos, funcionarios gubernamentales y organizaciones del sector privado, un ISAC puede ampliar el trabajo efectivo que se está realizando, cerrando colectivamente la brecha educativa y aumentando la atracción de talento para una fuerza laboral cibernética. Los ISAC ofrecen la oportunidad inigualable de satisfacer las necesidades únicas de América Latina y el Caribe, superando el simple intercambio de información para facilitar otras iniciativas importantes, como las oportunidades educativas y el desarrollo de la fuerza laboral.

[63] CEPAL, Latin American Economic Outlook 2020: Digital transformation for building back better, September 9, 2020.
[64] The World Bank, The Digital Economy Initiative for Latin America and the Caribbean, April 2024 https://www.worldbank.org/en/programs/de4lac.
[65] Hackers do Bem, About the Program, https://hackersdobem.org.br/o-programa.
[66] CEPAL, Latin American Economic Outlook 2020: Digital transformation for building back better, September 9, 2020, pg. 108.

INICIATIVAS EXISTENTES DE INTERCAMBIO DE INFORMACIÓN

Muchos países de LATAM han implementado iniciativas preliminares para fomentar un mayor intercambio de información. La mayoría de las iniciativas son a nivel nacional, y aunque algunas han dado pasos para incorporar la participación del sector privado, muchas carecen de la formalidad y el alcance de un verdadero ISAC. Esta sección ofrece una visión general de las diversas iniciativas existentes.

Red Federal de Gestión de Incidentes Cibernéticos de Brasil – En Brasil, las instituciones de la administración pública federal están obligadas a participar en la Red Federal de Gestión de Incidentes Cibernéticos, a través de la cual se comparte información sobre amenazas, incidentes y vulnerabilidades.[67] Las empresas públicas, las sociedades de capital mixto y sus filiales pueden unirse a la red de forma voluntaria.[68] Aunque la red está abierta a las empresas públicas, su objetivo principal es facilitar el intercambio de información entre las instituciones públicas federales.

Sin embargo, existen mecanismos alternativos en Brasil. Por ejemplo, en el sector de las telecomunicaciones, un grupo de trabajo establecido por Anatel utiliza una plataforma de intercambio de información sobre malware (MISP) para compartir información sobre amenazas y vulnerabilidades.[69] Además, organizaciones financieras, como la Federación de Bancos de Brasil, han informado de su participación en redes internacionales de intercambio de información, como la Red de Análisis e Intercambio de Información sobre Servicios Financieros (FS-ISAC). El sector financiero ha señalado que el intercambio de información entre todos los sectores de infraestructuras críticas podría automatizarse aprovechando el uso del MISP, por ejemplo.[70]

Belice – Las naciones más pequeñas de LATAM, como Belice, también han comenzado a priorizar y a comprometerse con un mayor intercambio de información. Belice publicó su Estrategia de Ciberseguridad 2020-2030, que incluye una prioridad declarada para "desarrollar una capacidad nacional de respuesta a incidentes y protección de la infraestructura de información crítica".[71] Dentro de esta área prioritaria, Belice desarrollará un diálogo con sectores clave en un "enfoque por fases para adoptar un protocolo de intercambio de información".[72]

---

[67] Global Cybersecurity Capacity Center, Cyber Capacity Review - Brazil, p. 46, Aug. 2023, https://www.gov.br/gsi/pt-br/ssic/eventos/CMMreportBrazil2023_finalversoemingls.pdf.
[68] Brazilian-American Chamber of Congress, Brazil creates cyber-attack response network, Jul 27, 2021, https://brazilcham.com/brazil-creates-cyberattack-response-network/.
[69] Global Cybersecurity Capacity Center, Cyber Capacity Review - Brazil.
[70] Ibid.
[71] Government of Belize, National Cybersecurity Strategy Towards a Secure Cyberspace 2020-2030, pg. 27,https://www.pressoffice.gov.bz/wp-content/uploads/2019/12/belize-cybersecurity-strategy-2020-2023.pdf (last accessed Jul. 25, 2024).
[72] Ibid.

Un ISAC regional complementaría estas iniciativas regionales y facilitaría una mayor resiliencia regional.

CSIRT Americas Network – La Organización de los Estados Americanos (OEA) gestiona una Red regional de Equipos de Respuesta a Incidentes de Seguridad Informática en las Américas (CSIRT), que promueve el intercambio de información sobre amenazas a la seguridad, proporciona asistencia técnica para reforzar los servicios de los CSIRT y ofrece formación a especialistas en ciberseguridad.[73] El CSIRT Americas Network demuestra la voluntad de los gobiernos regionales de participar en el intercambio de información y sirve de ejemplo fundacional para los intercambios de información dentro de la región. La red está dirigida principalmente a los CSIRT existentes en la región, pero también cuenta con socios industriales externos que colaboran con el grupo.

CSIRT Financiero (Asobancaria) – CSIRT Financiero está liderado por la Asociación Bancaria y de Entidades Financieras de Colombia, Asobancaria, una asociación sin fines de lucro representativa del sector financiero colombiano. Apoya a las instituciones financieras para anticipar y mitigar los riesgos derivados de las amenazas cibernéticas a través del intercambio de información y la cooperación con organizaciones nacionales e internacionales.[74] La visión del CSIRT es ser el punto de referencia del sector financiero para el intercambio de información sobre amenazas cibernéticas basado en los principios de confianza y ser el centro de investigación e innovación que fortalezca la prevención de amenazas para el sector. Esta iniciativa puede estar bien posicionada para servir como un ISAC oficial del sector financiero pan-LATAM que involucre a entidades de toda América Latina y el Caribe, más allá de Colombia.

República Dominicana "Simulacro Cibernético" – Durante el verano de 2023, la República Dominicana llevó a cabo su "Simulacro Cibernético" anual, que convocó a varias organizaciones dentro de la región y otras partes interesadas internacionales de los EE.UU. y Canadá.[75] El Simulacro Cibernético funcionó de manera similar a una sesión presencial de un ISAC, con el propósito de "ofrecer un espacio para el análisis y la discusión sobre las necesidades nacionales, acciones e iniciativas, además de la creación de capacidades a través de laboratorios de simulación de incidentes cibernéticos hacia la protección de las infraestructuras críticas nacionales, y la seguridad cibernética de la región, entre otros aspectos críticos nacionales importantes". Gobiernos, instituciones y/o CIRTs/CERTs nacionales colaboraron con técnicos y representantes en materia de ciberseguridad, y las sesiones de intercambio sirvieron de plataforma para la cooperación y los debates sobre ciberseguridad.[76]

---

[73] CSIRT Americas, https://csirtamericas.org/en (last accessed July 24, 2024).
[74] CSIRT Asobancaria, https://www.csirtasobancaria.com/quienes-somos (last accessed Oct. 28, 2024).
[75] ITU Publications, Cyberdrill for Americas-Dominican Republic 2023, June 19, 2023, https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Pages/EVENTS/2023/cyberdrill-23-Dominican-Republic.aspx#gsc.tab=0.
[76] ITU Publications, Cyberdrill for Americas-Dominican Republic 2023.

FIRST – El Foro de Equipos de Seguridad y Respuesta a Incidentes (FIRST) es una organización líder y reconocida a nivel mundial en respuesta a incidentes. FIRST reúne a una amplia variedad de equipos de seguridad y respuesta a incidentes de los sectores gubernamental, comercial y académico. Su objetivo fomentar la cooperación y la coordinación en la prevención de incidentes, estimular una reacción rápida ante los mismos y promover el intercambio de información entre sus miembros y la comunidad en general.[77] En la actualidad, FIRST cuenta con más de 700 miembros en África, las Américas, Asia, Europa y Oceanía. Aunque FIRST no se dedica exclusivamente a la región de LATAM, su sólida red de miembros debería aprovecharse para los esfuerzos posteriores de intercambio de información centrados en LATAM.

FEBRABAN – La Federación Brasileña de Bancos (FEBRABAN) se fundó en 1967 como una asociación sin ánimo de lucro que colabora con las partes interesadas con el fin de contribuir al desarrollo económico, social y sostenible de Brasil.[78] En 2020, se creó el Laboratorio de Ciberseguridad de FEBRABAN con el objetivo de facilitar la colaboración entre los equipos de los bancos asociados en acciones de prevención, identificación y lucha contra el cibercrimen. Esta iniciativa podría ser un punto de partida útil para mejorar la cooperación y el intercambio de información en el sector financiero de la región.

LACNIC – El Registro de Direcciones de Internet para LATAM es una organización internacional no gubernamental establecida en Uruguay en 2022. Su misión es administrar los recursos digitales de Internet en LATAM manteniendo estándares de excelencia y transparencia y promoviendo un modelo participativo para el desarrollo de políticas. LACNIC lidera la construcción permanente de la comunidad regional fortaleciendo las capacidades tecnológicas y la investigación aplicada para el desarrollo de una internet estable y abierta.[79]

LACNIC está gestionado y dirigido por una junta de directivos compuesta por siete miembros elegidos por sus miembros, un grupo de más de 12.500 entidades que operan redes y proveen servicios en 33 territorios de LATAM. LACNIC también administra un CSIRT, que realiza las "funciones de coordinación necesarias para fortalecer las capacidades de respuesta ante incidentes relacionados con los recursos de numeración de Internet (Ipv4, Ipv6), los números autónomos y la resolución inversa en América Latina y el Caribe, en el marco de los objetivos específicos establecidos por la misión de LACNIC orientados a lograr el fortalecimiento constante de una Internet segura, estable, abierta y en continuo crecimiento".[80]

---

[77] FIRST, https://www.first.org/ (last accessed Oct. 28, 2024).
[78] FEBRABAN, https://portal.febraban.org.br/paginas/10/pt-br/# (last accessed Nov. 27, 2024).
[79] LACNIC, https://www.lacnic.net/966/1/lacnic/acerca-de-lacnic (last accessed Oct. 28, 2024).
[80] CSIRT LACNIC, https://csirt.lacnic.net/acerca (last accessed Oct. 28, 2024).

Conclusión

La naturaleza fragmentada de las iniciativas de intercambio de información en América Latina subraya la urgente necesidad de un ISAC regional centralizado para abordar las amenazas cibernéticas en curso. Dada la vulnerabilidad de LATAM a los ataques cibernéticos, un ISAC regional brindaría una gran oportunidad para fortalecer la resiliencia cibernética y la alfabetización digital de LATAM y permitiría la colaboración con los ISAC existentes y los socios internacionales. Actualmente, la mayoría de los países de la región dependen de la ayuda mutua y la asistencia de socios internacionales para responder a las amenazas cibernéticas. Además, la respuesta a incidentes en LATAM varía, y algunos países tienen mecanismos de respuesta más avanzados que otros. La creación de un ISAC en LATAM ayudaría a agilizar la respuesta a incidentes en la región mediante la creación de una red fiable y segura para los homólogos que pueden compartir información actualizada sobre las amenazas identificadas, las mejores prácticas y otra información relevante. Con el tiempo, el ISAC también elevaría el conocimiento general sobre ciberseguridad del público de LATAM.

Los ISAC han demostrado su efectividad a nivel mundial, siendo los países mejor preparados aquellos que participan en tales iniciativas. Un ISAC en LATAM reduciría la dependencia de aliados externos, como EE.UU. y la UE, reforzando las capacidades locales de respuesta ante incidentes. El deseo de una iniciativa de este tipo ya existe, con esfuerzos preliminares de intercambio de información en marcha. Las redes de CSIRT existentes y las colaboraciones con ISAC experimentados pueden servir como modelos valiosos para establecer un ISAC en LATAM, integrando a las partes interesadas de la industria y el mundo académico para garantizar la visibilidad global de la información sobre amenazas.

Para maximizar su eficacia, LATAM debe considerar detenidamente los diferentes modelos de estructura y gobernanza de un ISAC. Debido a los diferentes niveles de madurez, un enfoque híbrido puede funcionar mejor para la región. LATAM podría comenzar con un modelo sectorial para los sectores más avanzados (por ejemplo, finanzas), ampliando al mismo tiempo las iniciativas existentes en los países. Las organizaciones con sede en LATAM que ya participan en ISAC ubicados en EE.UU. o la UE deberían aprovechar su experiencia para guiar el desarrollo de ISAC en LATAM. Estas organizaciones pueden desempeñar un rol fundamental en el fomento de la colaboración, el intercambio de conocimientos y la creación de capacidades a medida que se establecen nuevos ISAC específicos para la región. Los ISAC específicos de LATAM podrían proporcionar análisis y perspectivas regionales únicos, abordando las amenazas, vulnerabilidades y tendencias específicas del panorama digital de la región que pueden no ser totalmente captadas por los ISAC globales o no regionales. Este enfoque localizado permitiría un análisis de inteligencia sobre amenazas más específico y estrategias de respuesta a incidentes mejor adaptadas.

Establecer relaciones personales será esencial para generar confianza entre los participantes, y deberán asignarse los recursos adecuados para garantizar que las funciones y responsabilidades estén claramente definidas, permitiendo que el grupo produzca análisis significativos.

Los ISAC existen en todo el mundo y tienen un historial probado de eficacia a la hora de aumentar la resiliencia de la ciberseguridad. Un ISAC integra a todas las partes interesadas y puede ayudar a salvar las diferencias de madurez que existen entre tantas naciones de LATAM. Los esfuerzos destinados a mejorar el intercambio de información ya están en marcha en la región, pero tendrán que ser impulsados con recursos adicionales y ampliados para incorporar a todas las partes interesadas. Dado el estado de amplias brechas de madurez en la política de ciberseguridad, capacitación digital y educación de LATAM, los ISAC pueden beneficiar a la región. Específicamente, pueden proporcionar acceso a las lecciones aprendidas y la inteligencia de amenazas procesables para las entidades menos maduras, así como aumentar la resiliencia colectiva de la región frente a las rigurosas amenazas cibernéticas.

DIGI AMERICAS ALLIANCE MEMBERS

aws Apple CHECK POINT CISCO CLOUDFLARE CROWDSTRIKE fluid attacks we hack your software Google

kriptos LUMU METABASE Q netskope paloalto NETWORKS Resecurity

Santander Schneider Electric Telefónica tenable Trellix TREND MICRO

DIGI AMERICAS