DIGI AMERICAS LATAM CISO

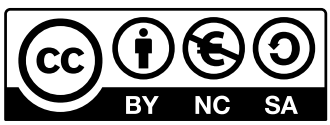
Duke UNIVERSITY

PREPARACIÓN CIBERNÉTICA

EN LOS SECTORES PÚBLICOS DE AMÉRICA LATINA:

LECCIONES DE LA PRIMERA LÍNEA

LATAMCISO REPORT 2024



CC BY-NC-SA: Esta licencia permite a los reutilizadores distribuir, remezclar, adaptar y construir sobre el material en cualquier medio o formato solo para fines no comerciales, y solo mientras se atribuya al creador. Si remezcla, adapta o construye sobre el material, debe licenciar el material modificado bajo términos idénticos.

Los contenidos expresados en este documento se presentan exclusivamente con fines informativos y no representan la opinión o posición oficial del Centro de Política y Derecho de Ciberseguridad, ni de ninguno de sus miembros.

Para obtener más información, póngase en contacto con **info@latamciso.com**

Créditos

Center for Cybersecurity Policy and Law

Belisario Contreras

Alexis Steffaro

Ines Jordan-Zoob

Universidad de Duke

David Hoffman

Camila Herrera

Lily Bermúdez

Daniela Pereira Salas

Andy Kotz

Lindsay Gross

Danielle Park

Ana Martínez

Hadrian González Castellanos

DIGI AMERICAS ALLIANCE MEMBERS

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

METABASE Q netskope paloalto NETWORKS Telefónica tenable

GRUPO RADICAL LUMU Trellix TREND MICRO Santander

Contenido

Resumen ejecutivo

El ransomware es una amenaza cibernética prevalente, particularmente en América Latina, donde los programas de ciberseguridad organizacional se encuentran en etapas formativas. Si bien numerosos factores pueden aumentar el riesgo de que los ataques de ransomware causen daños graves en la región, la falta de políticas y regulaciones de ciberseguridad en América Latina, como señala el Índice Nacional de Ciberseguridad (NCSI, por sus siglas en inglés), ha exacerbado aún más estos desafíos regionales.[I] Los ataques a la infraestructura crítica pueden perturbar significativamente el funcionamiento del gobierno y las empresas por igual y provocar un efecto dominó en los ciudadanos de las naciones latinoamericanas. Este informe utiliza la definición de infraestructura crítica del Instituto Nacional de Estándares y Tecnología (NIST): "Sistemas y activos, ya sean físicos o virtuales, tan vitales para el Estado que la incapacidad o destrucción de dichos sistemas y activos tendría un impacto debilitante en la seguridad, la seguridad económica nacional, la salud nacional o la seguridad pública, o cualquier combinación de esos problemas"[II]

Según el Banco Interamericano de Desarrollo (BID), solo siete de los 32 países latinoamericanos tienen planes para proteger su infraestructura crítica de ataques cibernéticos, y solo 20 cuentan con Equipos de Respuesta a Incidentes de Seguridad Cibernética (CSIRT, por sus siglas en inglés).[III] El nivel actual de preparación cibernética en la región sugiere que existe un déficit notable que debe abordarse.

El costo anual de los ciberataques en América Latina y el Caribe podría superar los $90 millones en 2025, con un promedio de más de 18,5 millones de ataques al año.[IV] Entre los incidentes más destacados se encuentra un ataque a Costa Rica en abril de 2022, que afectó a numerosas agencias gubernamentales y exigió un rescate de 10 millones de dólares. Otro ataque en mayo de 2022 tuvo como objetivo la Caja Costarricense de Seguro Social, causando interrupciones en sistemas críticos, incluida la finalización de los pagos de la seguridad social. Estos ataques provocaron que el país declarara el estado de emergencia, convirtiéndose en el primer país en utilizar fondos de emergencia debido a un ciberataque.[V] Del mismo modo, Colombia experimentó un importante ataque de ransomware por parte de un tercero a principios de septiembre de 2023, que interrumpió gravemente servicios vitales en todo el país. Este ataque afectó directamente a 20 entidades públicas, mientras que otras 78 entidades públicas y 762 empresas privadas se vieron afectadas indirectamente en América Latina, así como en otros países como Argentina, Panamá y Chile.[VI]

Las redes gubernamentales, ricas en información confidencial sobre sus ciudadanos, a menudo carecen de las mejores prácticas de seguridad, lo que las convierte en objetivos principales para los ataques cibernéticos. Este informe proporciona un análisis de las prácticas actuales de ciberseguridad, identifica cuellos de botella en la respuesta a incidentes y propone medidas efectivas para reforzar las defensas cibernéticas en América Latina. Además, este informe se centra en los enfoques que los gobiernos de la región pueden adoptar para ayudar a las organizaciones de sus países a mitigar el riesgo.

El estudio incluye análisis cualitativos y cuantitativos para examinar exhaustivamente los recientes eventos de ransomware en Colombia, Costa Rica, Chile y Panamá. Estos cuatro países se seleccionaron en función del grado en que habían experimentado una incidencia significativa de delitos cibernéticos, en particular ransomware. Además, fueron elegidos en función de su reciente marco regulatorio de ciberseguridad y su respuesta a incidentes significativos de ransomware. El aspecto cualitativo comprendió revisiones bibliográficas y entrevistas, centrándose en la comprensión de la efectividad y las deficiencias de las tácticas de respuesta. La revisión de la literatura incluyó documentación

de informes de incidentes, investigación académica y publicaciones gubernamentales. A través de esta revisión, se realizó un examen sobre la prevalencia de los ataques de ransomware en los cuatro países, así como un análisis de sus respectivas políticas nacionales de ciberseguridad y los desafíos de ciberseguridad a los que se enfrentan.

Las entrevistas con funcionarios gubernamentales proporcionaron información sobre el panorama de la respuesta a incidentes, las lecciones aprendidas y las mejores prácticas. Los funcionarios del gobierno variaban tanto en posición como en agencia. Los cargos de los entrevistados iban desde directores nacionales de ciberseguridad y analistas de ciberseguridad hasta directores de gestión de riesgos y transformación digital. Trabajan en muchas agencias gubernamentales diferentes dentro de los países antes mencionados, incluidos los ministerios de tecnología y las embajadas. Los temas abarcaron las respuestas de los gobiernos, las políticas existentes, los desafíos y el potencial de los marcos de gestión de riesgos (RMF) y las soluciones en la nube. El análisis cuantitativo consistió en una encuesta que tenía como objetivo recopilar perspectivas sobre la eficacia de los RMF, como el Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST CSF), y el impacto de la migración de las operaciones informáticas a los servicios en la nube en la reducción de los riesgos de ransomware. La encuesta utilizó opciones de respuesta de selección múltiple para aumentar las tasas de respuesta y fue diseñada para ser simple y rápida. Los encuestados comprendieron a más de 150 personas en puestos de alto nivel en los sectores público y privado, así como en la sociedad civil y la academia que provenían de países como Colombia, Argentina, Costa Rica, Chile y Guatemala. Los hallazgos combinados, que se centran en los RMF y la adopción de la nube pública, tienen como objetivo informar las estrategias para mejorar la respuesta a incidentes y salvaguardar la infraestructura crítica en los países de América Latina.

Una conclusión clave de este estudio es que el entorno de riesgo de ciberseguridad en constante cambio es difícil de gestionar. Muchos países de la región de América Latina tienen capacidades de ciberseguridad relativamente nuevas, pero no por ello menos prometedoras. Los hallazgos de este informe, compilados a partir de la literatura, entrevistas y una encuesta a actores clave en la región, indican una resiliencia sustancial a los ataques en varios países de América Latina. Si bien cada país tiene diferentes antecedentes y capacidades cibernéticas, todos respondieron a los ataques y otros desafíos de manera sólida, teniendo en cuenta las limitaciones de sus recursos.

Los hallazgos clave destacan posibles áreas de oportunidad de mejora, como una escasez significativa de profesionales de TI capacitados, mecanismos inadecuados de respuesta a incidentes y una falta de políticas de ciberseguridad cohesivas en varios sectores. Las inversiones en ciberseguridad no siguen el ritmo del aumento de la digitalización y sus riesgos asociados, especialmente en el sector gubernamental. Abordar los desafíos regionales planteados por la prevalencia de amenazas de ransomware es imperativo debido a la etapa inicial de los programas de ciberseguridad organizacional en América Latina y la ausencia de políticas y regulaciones de ciberseguridad para la infraestructura crítica.

Dado que los ataques a la infraestructura crítica pueden tener consecuencias de gran alcance en las operaciones gubernamentales, la continuidad del negocio y el bienestar público, las recomendaciones de este estudio se centran en: (1) reforzar la inversión en el desarrollo de la fuerza laboral, (2) establecer RMF voluntarios, (3) invertir en infraestructura y tecnologías de ciberseguridad, como la infraestructura de ciberseguridad basada en la nube, y (4) formar sistemas centralizados de gestión e informes de ciberseguridad para mitigar estos riesgos de manera efectiva.

ATAQUES DE RANSOMWARE EN AMÉRICA LATINA

CASO DE ESTUDIO:

COLOMBIA

Introducción

El fortalecimiento de la ciberseguridad se ha convertido en un tema de profunda importancia estratégica para las naciones de todo el mundo. Para países como Colombia, que ocupa el tercer lugar en el ranking de países sudamericanos que más ataques de ransomware han sufrido y al mismo tiempo aspira a convertirse en una fuerza dominante dentro de la industria tecnológica, es imperativo desarrollar la resiliencia nacional frente a los riesgos cibernéticos.[VII] Como tal, esta sección examina el panorama de ciberseguridad, las políticas, los ataques cibernéticos, los desafíos y las oportunidades futuras de Colombia. También analiza los hallazgos de las entrevistas realizadas con funcionarios del gobierno después del ataque de ransomware en septiembre de 2023 y las lecciones aprendidas del incidente.

Colombia define la infraestructura crítica de la siguiente manera. (1) La "Estrategia de Seguridad: Infraestructura Crítica Nacional 2022-2032" describe la infraestructura crítica como los sistemas físicos y virtuales que permiten la operación de servicios esenciales y básicos a nivel social, económico, ambiental y político.[VIII] Una alteración o interrupción de estos sistemas debido a la naturaleza o al hombre podría tener consecuencias negativas para los gobiernos, los estados y los ciudadanos, ya que no podrían realizar sus actividades diarias, lo que llevaría a la parálisis de la nación afectada. De igual forma, (2) el Decreto 338 de 2022 define la infraestructura crítica como "los sistemas y activos, físicos o virtuales, apoyados en las Tecnologías de la Información y las

Comunicaciones, cuyo impacto significativo tendría un impacto grave en el bienestar social o económico de los ciudadanos, o en el funcionamiento efectivo del gobierno o la economía".[IX]

Panorama de la Política de Ciberseguridad en Colombia

Colombia gestiona sus propias políticas de seguridad digital a través de una serie de documentos del Consejo Nacional de Política Económica y Social (CONPES), así como de leyes y reglamentos pertinentes en el ordenamiento jurídico. Un hito importante se logró con la aprobación de la Ley 1273 en 2009.[X] Esta ley estableció disposiciones para combatir los delitos informáticos, incluido el acceso no autorizado al sistema, la destrucción de datos y la interrupción de los servicios digitales.[XI] Al definir las actividades cibernéticas ilícitas, la Ley 1273 promovió un entorno digital más seguro y confiable.[XII] El cumplimiento de sus estatutos es esencial para las entidades del sector público y privado a medida que Colombia continúa su camino hacia la transformación digital.

El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) cuenta con tres planes principales de seguridad digital: CONPES 3701, 3854 y 3995. En 2011, Colombia introdujo el Marco Nacional de Ciberseguridad, CONPES 3701, para proporcionar directrices y mejores prácticas para proteger la infraestructura crítica y los sistemas de información centrales.[XIII] El marco estableció el Comité Nacional de Ciberseguridad para alinear los esfuerzos interinstitucionales y el Equipo Nacional de Respuesta a Incidentes de Seguridad Informática (CSIRT) para detectar y mitigar los ciberataques. En 2012, siguiendo los lineamientos establecidos en el CONPES 3701, Colombia también fundó su primera unidad cibernética conectando tres entidades independientes que fueron creadas para realizar tareas distintas en el dominio del ciberespacio: el Equipo de Respuesta a Emergencias Informáticas (ColCERT) del Ministerio de Defensa, el Comando Cibernético Conjunto (CCOC) y el Centro Cibernético de la Policía Nacional (CCP).[XV] El objetivo era diseñar un esfuerzo más coordinado entre las agencias.

El CONPES 3854, promulgado el 11 de abril de 2016, estableció la Política Nacional de Seguridad Digital, que creó las condiciones para que diversos actores gestionaran los riesgos de seguridad digital en sus actividades socioeconómicas y fomentó la confianza en el entorno digital.[XVI] Una contribución significativa a esta política fue el desarrollo de estrategias que establecían un marco institucional para la seguridad digital con un enfoque preventivo en lugar de respuestas reactivas a posibles amenazas. Esta política también reconoce el enfoque previo del país en la ciberseguridad para la defensa, la seguridad y el delito cibernético y amplía su alcance para incluir la gestión de riesgos, lo que refleja la creciente importancia de las tecnologías de la información y la comunicación (TIC) para el progreso socioeconómico. Además, la política introdujo el rol del coordinador nacional de seguridad digital, quien supervisó el Consejo Presidencial para la Transformación Digital, Gestión y Cumplimiento de la Presidencia de la República.

Se realizaron mejoras adicionales a través del Decreto 620 de 2019, que reglamenta la Ley 1273 al tiempo que aborda las amenazas emergentes, como los ataques de

denegación de servicio y las brechas de protección de infraestructura crítica.[XVII] El Decreto 620 de 2020 estableció lineamientos específicos para la implementación de medidas de ciberseguridad en el sector privado para clarificar y ampliar las obligaciones legales junto con los cambios tecnológicos.[XVIII]

En materia de protección de datos, Colombia promulgó la Ley 1581 de 2012 y el Decreto 1377 para proteger los derechos constitucionales a la privacidad.[XIX] Este marco integral impone obligaciones con respecto a los flujos de datos personales, los controles de acceso y las notificaciones de violación en todos los sectores. Colombia también instituyó el Registro Nacional de Bases de Datos para permitir la notificación de incidentes cibernéticos entre empresas. Mientras que los CSIRT sectoriales ayudan a industrias como las finanzas, las telecomunicaciones y la energía, el CSIRT gubernamental debe superar las limitaciones presupuestarias y de continuidad. La propuesta de una agencia nacional de seguridad digital tiene como objetivo abordar estos desafíos de capacidad institucional.

En Colombia, el CONPES 3995 de 2020, el Decreto 338 de 2022 y el Decreto 762 de 2022 son las políticas y leyes nacionales de ciberseguridad vigentes más recientes. CONPES 3995, la Política Nacional de Confianza y Seguridad Digital, establece medidas para desarrollar la confianza digital a través de mejoras en la seguridad digital. También busca generar condiciones de seguridad y convivencia para preservar y potenciar los intereses nacionales, la independencia, la soberanía y la integridad dentro del Estado.[XX] El Decreto 338 de 2022 establece lineamientos generales para fortalecer la gobernanza de la seguridad digital en Colombia. El decreto también crea el Modelo de Gobernanza de Seguridad Digital, que tiene como objetivo fortalecer la gestión de los riesgos de seguridad digital para los servicios esenciales y las infraestructuras cibernéticas críticas en Colombia. Adicionalmente, el Decreto modifica la organización y funcionamiento del grupo de trabajo interno de respuesta a emergencias cibernéticas de Colombia, ColCERT.[XXI] El Decreto 767 de 2022, Política de Gobierno Digital, tiene como objetivo mejorar la eficiencia, transparencia y calidad de los servicios prestados por el Estado. Esta política defiende tres pilares fundamentales: la arquitectura, la seguridad y privacidad de la información y los servicios digitales al ciudadano.[XII] Además, se ha introducido un nuevo facilitador, "Cultura y apropiación" (un facilitador de tecnología es un término utilizado para describir una tecnología o un conjunto de tecnologías que proporcionan una plataforma o base para el desarrollo de otras tecnologías, productos o servicios.[XIII]). Este facilitador tiene por objeto mejorar las capacidades de las entidades y los grupos de interés con mandato, velando por su aptitud para utilizar y aprovechar las TIC para el acceso y la utilidad.

En general, Colombia ha fortalecido sus medidas de ciberseguridad a través de la implementación de varias leyes y políticas, comenzando con la Ley 1273 en 2009 y continuando con la legislación más reciente, como el Decreto 620 de 2019 y el Decreto 338 de 2022. Estas políticas buscan proteger la integridad del estado, promover la confianza digital y reforzar las defensas contra los ataques cibernéticos. A medida que Colombia avanza en su transformación digital, el cumplimiento de estos estándares es crucial para las organizaciones de los sectores público y comercial.

Participación y contribuciones del sector privado

Los ciberataques se han vuelto omnipresentes y afectan a muchos tipos de sistemas, desde la infraestructura corporativa hasta los correos electrónicos, las aplicaciones y los datos almacenados en la nube privada. En 2023 se registraron aproximadamente 29.000 ataques a infraestructuras corporativas, más de 8.000 ataques relacionados con el robo de información y bases de datos, y alrededor de 16.000 incidentes vinculados a redes sociales y correos electrónicos. [XXIV]

En Colombia, el sector privado contribuye activamente a los esfuerzos de ciberseguridad, priorizando la protección de los activos digitales y la información sensible.[XXV] Las organizaciones privadas se adhieren a estándares y regulaciones internacionales específicas, como la Política de Ciberseguridad y la Política de Seguridad Digital, lo que garantiza el cumplimiento de la protección contra las amenazas cibernéticas.[XXVI] Las colaboraciones con organismos gubernamentales, incluidos ColCERT, CCOC y el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), se centran en el avance de los marcos y la integración de medidas de ciberseguridad en sectores críticos.[XXVII] Muchas organizaciones privadas participan activamente en la respuesta a incidentes a través de CSIRT en sectores críticos, lo que garantiza la resiliencia frente a las amenazas cibernéticas.[XXVIII] Estos esfuerzos demuestran que el sector privado, como las empresas multinacionales de tecnología, está profundamente comprometido con el fortalecimiento de la ciberseguridad de Colombia.

Colaboraciones internacionales

En Colombia se están realizando importantes esfuerzos para avanzar en la reducción de la brecha digital entre los países desarrollados. Algunas de estas normas internacionales que se tienen como referencia de facto son las emitidas por el Instituto Nacional de Estándares y Tecnología (NIST; Comercio, 2018) e ISO 27001.[XXIX] Además, Colombia aprobó la Ley 1928 de 2018,[XXX] que llevó a la adopción del Convenio sobre Ciberdelincuencia del Consejo de Europa, también conocido como Convenio de Budapest.[XXXI] El Convenio de Budapest es el primer acuerdo internacional destinado a combatir la ciberdelincuencia, o delitos relacionados con las computadoras e Internet, mediante la adecuación de las leyes nacionales, la mejora de los métodos de investigación y el fomento de la cooperación internacional.[XXXII] Esta incorporación introdujo en el marco jurídico colombiano todas las obligaciones relacionadas con el delito cibernético previstas en el Convenio de Budapest. El 16 de marzo de 2020, el Consejo de Europa anunció oficialmente que Colombia se había adherido al Convenio de Budapest, convirtiéndose así en el 65° país en adherirse.[XXXIII]

En 2020, Colombia implementó un tratado de libre comercio (TLC) con Israel, que había sido firmado en 2014. El TLC con Israel promovió la colaboración en sectores como la tecnología, la innovación, la ciberseguridad y el crecimiento agrícola e industrial. Este acuerdo es relevante en el contexto del objetivo del gobierno de hacer de la innovación la base de la economía colombiana.[XXXIV] Además, en 2022, Israel hizo una contribución significativa a la mejora de las capacidades de

ciberseguridad en América Latina, particularmente en Colombia y el Caribe. Este aporte de $2 millones fue entregado al Banco Interamericano de Desarrollo, que liderará la iniciativa de ciberseguridad.[XXXV]

Colombia se ha involucrado activamente en el escenario internacional, demostrando liderazgo y participación en diversos foros cruciales. En 2018, el país logró un hito importante al ser elegido como presidente inaugural del Grupo de Trabajo sobre Medidas Cibernéticas de Fomento de la Confianza en la Organización de los Estados Americanos (OEA).[XXXVI] Este nombramiento subraya el compromiso de Colombia de promover la cooperación y el diálogo en temas de ciberseguridad dentro de la región. Además, Colombia mantiene una participación activa en organismos internacionales, como la Organización de las Naciones Unidas (ONU) y la Unión Internacional de Telecomunicaciones (UIT), donde contribuye a las discusiones e iniciativas globales relacionadas con la tecnología, las telecomunicaciones y la ciberseguridad.[XXXVII] Además, Colombia colabora con instituciones financieras multilaterales, como el Banco Interamericano de Desarrollo (BID), el Banco Mundial y la Corporación Andina de Fomento (CAF), para abordar los desafíos del desarrollo y avanzar en proyectos que promuevan el crecimiento económico y la sostenibilidad tanto a nivel nacional como en toda la región. A través de estos compromisos, Colombia ha demostrado su dedicación a fomentar la colaboración, compartir las mejores prácticas y abordar los desafíos globales en la era digital.

Retos de ciberseguridad en Colombia

En los últimos años, Colombia, al igual que el resto de la región, se ha enfrentado a una mayor vulnerabilidad a las amenazas cibernéticas, que han sido impulsadas por los rápidos avances tecnológicos y la digitalización acelerada por la pandemia de COVID-19. Este aumento de la digitalización y la penetración de Internet eleva la probabilidad de posibles vulnerabilidades y ciberataques si no va acompañado de medidas de seguridad adecuadas para proteger el entorno digital ampliado. En 2021, Colombia se ubicó entre los países latinoamericanos más atacados por actores maliciosos, lo que refleja una preocupante tendencia al alza.[XXXVIII] Un estudio realizado entre 2022 y 2023 por la Cámara Colombiana de Informática y Telecomunicaciones reveló que las víctimas registraban una denuncia por incidente cibernético cada ocho minutos.[XXXIX] En los últimos dos años, Colombia experimentó dos grandes ataques de ransomware.

En primer lugar, en diciembre de 2022, el sistema de salud de Colombia sufrió un duro golpe por una filtración de datos.[XL] El perpetrador utilizó el ransomware RansomHouse para comprometer las redes de Keralty, un gran proveedor de atención médica.[XLI] La violación expuso los datos de salud confidenciales de miles de usuarios, incluidos nombres, direcciones, números de seguro social y registros médicos.[XLII] Esta brecha en la atención médica tuvo impactos en cascada en todo el país, ya que fallaron los sistemas de programación de los hospitales, lo que provocó

tiempos de espera más largos para los pacientes o la pérdida de acceso a servicios esenciales por completo.[XLIII] Estimulado por este ataque, Keralty invirtió mucho en nuevas medidas de seguridad y personal experto para reforzar sus defensas.[XLIV]

En segundo lugar, en septiembre de 2023, el proveedor de servicios de Internet de Colombia, IFX Networks, informó haber sido víctima de un ataque de ransomware.[XLV] Alrededor de 78 entidades estatales colombianas y 762 empresas privadas se vieron afectadas por el ataque, entre ellas[XLVI] el Ministerio de Salud y Protección Social, el Poder Judicial del país y la Superintendencia de Industria y Comercio.[XLVII] Este incidente tuvo un impacto significativo en las operaciones diarias del gobierno colombiano. Por ejemplo, dos millones de procesos judiciales programados fueron suspendidos por siete días porque los portales web del Poder Judicial estaban completamente congelados y no había forma de determinar el estado de los procedimientos en el sistema.[XLVIII] Muchos centros de salud también perdieron sus servicios en línea, lo que significa que los pacientes no podían hacer citas médicas u obtener sus recetas porque los doctores no podían acceder a los registros médicos de los pacientes.

El asesor presidencial para la transformación digital dirigió el puesto de comando cibernético unificado del gobierno colombiano, que supervisó la respuesta al ataque de 2023. El asesor envió aproximadamente nueve boletines informativos antes de que terminara el evento y el país volviera a la normalidad. El asesor presidencial también se aseguró de que las plataformas y aplicaciones afectadas de las entidades continuaran funcionando correctamente durante el evento. Según un comunicado de prensa público de IFX, IFX pudo recuperar el 90% de la información en el décimo día después del ataque. Muchos funcionarios del gobierno expresaron que este ataque fue considerado el "más grande contra la infraestructura en Colombia en los últimos años" y ha llevado a la legislatura del país a aprobar un nuevo ministerio y crear la Agencia Nacional de Ciberseguridad y Asuntos Espaciales. [XLIX]

En noviembre de 2023, se presentaron dos proyectos de ley a la legislatura colombiana para crear una autoridad técnica y especializada en seguridad digital.[L] El primer proyecto de ley, radicado el 24 de julio, proponía la creación de la Agencia Nacional de Seguridad Digital (ANSD), liderada por congresistas. El segundo proyecto de ley fue liderado por el Ministerio de Tecnologías de la Información y las Comunicaciones y alineado con la estrategia de ciberseguridad del Ministerio presentada a principios de ese mes. Este proyecto de ley era más amplio que el primero, ya que requería una agencia de seguridad digital y espacial (ANSDAE). Estas propuestas para la gestión de la seguridad digital en Colombia difieren en su vinculación organizacional y alcance de responsabilidades. El MinTIC sugiere crear la Agencia Nacional de Seguridad Digital y Asuntos Espaciales bajo la presidencia, lo que podría otorgarle "poderes extraordinarios". En contraste, la propuesta de los senadores recomienda que la agencia dependa del Ministerio

de TIC para supervisar las asignaciones de recursos existentes y evitar gastos adicionales. Además, la propuesta de los senadores hace hincapié en obligar tanto a las entidades públicas como a las privadas a revelar los riesgos de ciberataques para el apoyo de la agencia, mientras que la propuesta del MinTIC carece de tales obligaciones.

Si bien Colombia ha desarrollado una base legal y política para la ciberseguridad nacional, persisten los desafíos para lograr la plena implementación y abordar las brechas de capacidad. Para navegar por el cambiante panorama de amenazas, se necesitan esfuerzos sostenidos para mejorar la experiencia técnica, mejorar el intercambio de información, proporcionar claridad regulatoria y alinear las direcciones estratégicas.

Subrayar la importancia de la ciberseguridad y pedir una gobernanza vinculante

En las entrevistas realizadas, hubo un consenso unánime sobre los importantes riesgos cibernéticos en torno a la protección de datos sensibles y la seguridad nacional en Colombia, especialmente tras el gran ataque de ransomware experimentado en septiembre de 2023. Este consenso puso de relieve la alineación en torno a la importancia fundamental de la ciberseguridad como prioridad nacional para el enfoque y la inversión sostenida. Los participantes hicieron hincapié en la importancia de promulgar leyes y políticas integrales y aplicables y de formalizar la gobernanza nacional de la ciberseguridad. Del mismo modo, los entrevistados coincidieron en que las normas vinculantes y la coordinación institucional eran medidas esenciales para impulsar la rendición de cuentas, la transparencia y la eficacia en la preparación y la respuesta.

Lidiando con las brechas de respuesta a incidentes

Un hallazgo importante fue que la respuesta a incidentes es actualmente ineficiente. Los participantes mencionaron las dificultades actuales para detectar ataques de forma rápida y precisa y determinar su origen en medio de la complejidad de las amenazas cibernéticas. Además, los participantes hicieron hincapié en las complicaciones para evaluar y contener los impactos posteriores, ya que los ataques que se propagan a los sistemas interconectados son cada vez más difíciles de rastrear. Estas deficiencias de respuesta sistémica indican áreas importantes en las que se requiere desarrollar capacidades para mitigar los riesgos cibernéticos. Además, las aportaciones de los entrevistados, junto con las respuestas de la encuesta, que se examinarán en una sección posterior, pusieron de relieve la necesidad de mantener la comunicación dentro de las organizaciones y entre ellas. En concreto, muchos entrevistados indicaron la necesidad de implementar medidas sencillas de ciberseguridad que permitan una preparación y contención más eficaz de los ataques cuando se produzcan.

Reconocer la educación como piedra angular esencial

Los entrevistados también coincidieron de manera uniforme en la necesidad de ampliar los programas de capacitación y cultivar la conciencia cibernética en las entidades del sector público y privado, así como en la población en general en Colombia. Por lo tanto, el desarrollo del talento y la cultura en torno a la ciberseguridad surge como una inversión fundamental para impulsar la madurez, la resiliencia y la reducción de riesgos a lo largo del tiempo tanto en las organizaciones como en los ciudadanos. Los entrevistados hicieron hincapié en que los programas informáticos y los sistemas de respuesta robustos por sí solos no pueden mitigar suficientemente el riesgo cibernético y permitir una respuesta eficaz a los incidentes. También se requiere una inversión significativa en el cultivo del talento humano y la experiencia en ciberseguridad en todos los equipos encargados de la detección, contención y recuperación de los ataques.

Perspectivas sobre la adopción de la nube para disminuir los riesgos de ciberseguridad

Numerosos participantes destacaron la importancia y los beneficios de trabajar con los mejores proveedores de servicios de comunicaciones (CSP) para gestionar los riesgos de ciberseguridad. Los participantes también destacaron que los beneficios de seguridad deben considerarse junto con la capacidad de controlar cómo se accede a los datos y cómo se procesan.

Evolución de los marcos de ciberseguridad centrados en el Instituto Nacional de Estándares y Tecnología (NIST)

Las entrevistas revelaron que es necesaria la evolución de las estrategias y regulaciones de ciberseguridad para hacer frente a las nuevas amenazas. Un entrevistado se refirió específicamente a las iniciativas continuas para fomentar el uso y la comprensión de la iteración más reciente del marco NIST 2.0. Además, el énfasis en procesos de desarrollo legislativo más amplios sugiere un enfoque proactivo destinado a adecuar la gobernanza de la ciberseguridad de Colombia a los marcos de gestión de riesgos (RMF). De este modo, se permitirá la integración de las mejores prácticas y la preservación de la flexibilidad frente a la evolución de las técnicas de ataque.

Abrazar la colaboración internacional

Finalmente, los participantes expresaron un consenso unánime para ampliar los mecanismos internacionales de intercambio técnico, asistencia y cooperación para ayudar a expandir las capacidades y el aprendizaje colectivo en la gestión de las sofisticadas amenazas cibernéticas globales que afectan a Colombia. Este hallazgo revela una conciencia de que, si bien muchas vulnerabilidades requieren el desarrollo de capacidades internas, los entornos de amenazas trascienden las fronteras y pueden gestionarse de manera más efectiva con un esfuerzo internacionales.

CASO DE ESTUDIO:

COSTA RICA

Introducción

Costa Rica ha adoptado gradualmente un enfoque estratégico para la cooperación internacional en materia de ciberseguridad, aprovechando los programas regionales, los tratados, las asociaciones bilaterales y la asistencia extranjera para desarrollar capacidad de manera sistemática. Esta sección proporciona un análisis del entorno, las leyes, las amenazas, las dificultades y las perspectivas de ciberseguridad de Costa Rica. A medida que avanza la digitalización, surgen soluciones específicas para proteger la seguridad nacional, los intereses empresariales y los derechos de los ciudadanos. Estas soluciones pueden basarse en un conocimiento detallado del panorama de la ciberseguridad de Costa Rica, especialmente después del gran ataque de ransomware en 2022.

Visión general de la política de ciberseguridad en Costa Rica

En 2012, la Ley de Delitos Cibernéticos 9048, la primera ley integral del país destinada a combatir el delito cibernético y la piratería informática, marcó el inicio de los esfuerzos serios de Costa Rica en materia de ciberseguridad. Esta ley estableció marcos legales para criminalizar y perseguir diferentes violaciones cibernéticas, como el acceso no autorizado al sistema, el sabotaje de datos y sistemas, y el fraude electrónico. La introducción de la ley provocó el establecimiento de unidades especializadas de policía cibernética y capacidades de enjuiciamiento de delitos cibernéticos dentro del sector público.[LII] Ese mismo año, se creó el Equipo de Respuesta a Incidentes de Seguridad Informática de Costa Rica (CSIRT-CR) bajo el Decreto Ejecutivo 37052-MICITT.[LIII] Este decreto designó al CSIRT-CR como el organismo responsable de coordinar todos los asuntos relacionados con la seguridad informática y cibernética. Además, facultó al CSIRT-CR para mantener un equipo de expertos en seguridad de las TIC encargados de prevenir y abordar los incidentes que afectan a las instituciones gubernamentales. La misión del CSIRT-CR incluye la implementación y gestión de medidas tecnológicas destinadas a reducir el riesgo de ataques a los sistemas comunitarios, integrar los sistemas de seguridad cibernética y las tecnologías de la información en los marcos de protección del gobierno central y las entidades autónomas, y mitigar los riesgos y amenazas cibernéticas.

En 2011, Costa Rica aprobó y publicó la Ley 9868, que posteriormente entró en vigencia en 2012. Esta ley, denominada Ley de Protección de la Persona Frente al Tratamiento de Sus Datos Personales, se ha mantenido inalterada desde su publicación.[LIV] La ley se aplica a los datos personales que aparecen en las bases de datos automatizadas y manuales de organizaciones públicas y privadas y a cualquier uso posterior de estos datos.[LV]

En 2014, Costa Rica introdujo una política nacional de ciberseguridad fundamental con un plan nacional de desarrollo que identificó los objetivos centrales de los sectores público y privado, incluido el fomento de una cultura de concientización sobre el riesgo cibernético, la protección de la infraestructura vital y la mejora de la preparación para incidentes.[LVI] Además, se impusieron obligaciones de notificación de incidentes cibernéticos a los operadores de sistemas críticos para facilitar el monitoreo de amenazas.[LVII]

De igual forma, en 2017, el Gobierno de Costa Rica desarrolló su Estrategia Nacional de Ciberseguridad 2017-2021, la cual estableció un marco institucional que avanzó en sus funciones y actividades bajo el liderazgo del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) y el CSIRT-CR.[LVIII] Esta estrategia esbozó una visión estratégica y prioridades para fortalecer sistemáticamente las defensas cibernéticas en las agencias gubernamentales y los operadores de infraestructura crítica. Además, la estrategia nacional definió la infraestructura crítica como "los sistemas y redes de información

que, si se ven comprometidos, podrían afectar significativamente la salud de los ciudadanos, la seguridad física y operativa, la economía, el bienestar o el funcionamiento efectivo del gobierno y la economía del país". Además, en la estrategia se hizo hincapié en la necesidad de delimitar la infraestructura crítica del país y establecer un comité de formulación de políticas integrado por representantes de entidades públicas y privadas clasificadas como infraestructuras críticas.

En noviembre de 2023, el gobierno de Rodrigo Chaves introdujo un nuevo plan de ciberseguridad, la Estrategia Nacional de Ciberseguridad 2023-2027, tras los ciberataques de 2022, que provocaron el estado de emergencia en el país.[LIX] El esfuerzo presentó una visión estratégica que refuerza el liderazgo del gobierno nacional y pretende unir a todos los actores en torno a los derechos humanos.[LX] Esta estrategia describe cómo mejorar la protección de la infraestructura y la ciberresiliencia nacional, impulsar la gobernanza de la ciberseguridad, modificar el marco ciberjurídico, apoyar el ecosistema de ciberseguridad y colaborar activamente en la esfera digital.[LXI]

Participación y contribuciones del sector privado

El sector privado también se ha visto afectado por el aumento de los ataques cibernéticos en Costa Rica. En agosto de 2020, se creó el primer clúster de ciberseguridad del país, la iniciativa Cybersec Costa Rica Cluster, para posicionar a Costa Rica como líder en la región centroamericana.[LXII] La iniciativa es una alianza público-privada entre empresas, cámaras, academia e instituciones públicas que presenta el primer gran clúster internacional de ciberseguridad de la región para mejorar la competitividad del país.[LXIII]

En febrero de 2022, el Decreto Ejecutivo 43425-MEIC-MTSS estableció el Programa Nacional de Clusters (PNC) como asunto de interés público.[LXIV] El decreto faculta a los ministerios para alinear los marcos normativos y las iniciativas, lo que permite a la PNC impactar positivamente en el desarrollo productivo y la generación de empleos. El modelo de clústeres representa un enfoque innovador para una asociación público-privada, que hace hincapié en la colaboración y la confianza entre las partes interesadas.[LXV] Entre los participantes se encuentran miembros de Digi Americas, destacando a las principales empresas multinacionales de diferentes sectores, como Amazon Web Services y Cisco.[LXVI] El clúster se centra estratégicamente en el desarrollo y fortalecimiento del ecosistema de ciberseguridad y en la mejora de la fuerza laboral de ciberseguridad. Costa Rica es el primer país latinoamericano con un programa PNC declarado por decreto ejecutivo.[LXVII]

Colaboraciones Internacionales

Costa Rica ha buscado activamente asociaciones internacionales de ciberseguridad durante más de una década, comenzando con el Programa de Seguridad Cibernética de la OEA a fines de la década de 2000.[LXVIII] Este programa incluyó capacitación cibernética y desarrollo de capacidades para los sectores público y privado de Costa Rica. En 2019, Costa Rica reconoció el liderazgo del Grupo de Trabajo de la OEA en la coordinación de la respuesta regional a incidentes y el establecimiento de marcos de acción de cooperación para las amenazas

cibernéticas.[LXIX] En 2017, Costa Rica se convirtió en signataria del Convenio de Budapest. Costa Rica también sigue participando activamente en el foro del Grupo de Trabajo de Composición Abierta de las Naciones Unidas (GTCA) sobre gobernanza cibernética y se ha comprometido a participar de manera continua hasta 2025.[LXX] En el GTCA 2022, Costa Rica reiteró su compromiso con la aplicación del derecho y las normas internacionales, incluidos los principios de proporcionalidad y humanidad, al uso de las TIC por parte del Estado.[LXXI]

En cuanto a la colaboración específica con otros países, el Japón apoyó la pronta elaboración por parte de Costa Rica de un CSIRT nacional a través del Programa de Cooperación Internacional del Japón (JICA).[LXXII] Además, Costa Rica firmó un memorando de entendimiento (MOU) con Israel [LXXIII] sobre capacidades cibernéticas y cooperación en materia de ciberseguridad.[LXXIV] Este memorando fue beneficioso durante el ataque de ransomware en 2022, cuando Israel proporcionó inteligencia relevante y aumentó la comprensión del gobierno costarricense sobre qué sistemas fueron atacados y posteriormente cerrados.[LXXV] Otra colaboración clave fue con España, que también brindó soporte técnico y donó herramientas de protección durante el ataque de ransomware en 2022.[LXXVI] En 2023, Estados Unidos anunció planes para proporcionar 25 millones de dólares en asistencia a Costa Rica para establecer un centro de operaciones de ciberseguridad para 2026 en respuesta al ataque de ransomware, que proporcionará equipos avanzados, capacitación especializada y ayuda logística al Ministerio de Seguridad Pública de Costa Rica.[LXXVII] Además, Costa Rica ha formalizado acuerdos cibernéticos con República Dominicana y Panamá.[LXXVIII] A través de memorandos de entendimiento, el MICITT de Costa Rica y sus contrapartes están intercambiando mejores prácticas y políticas para alinearse con la Estrategia Nacional de Ciberseguridad de Costa Rica.

Costa Rica sigue siendo un punto focal para el desarrollo de capacidades de ciberseguridad en la región. En septiembre de 2024, el Centro de Políticas y Leyes de Ciberseguridad (CCPL), junto con su Alianza Digi Americas, organizarán la Cumbre de Directores de Seguridad de la Información de América Latina (LATAM CISO) 2024 en Guanacaste, Costa Rica. Esta exclusiva cumbre reúne a los más altos líderes, operadores e influencers de ciberseguridad de Iberoamérica para debatir sobre las amenazas y tendencias más críticas y desafiantes del mundo digital. Los temas incluirán la protección de infraestructuras críticas, la identidad digital y la privacidad, el 5G, las amenazas y tendencias emergentes, y la evolución y los desafíos de la industria de la tecnología financiera (fintech), entre otros temas relevantes. La Comisión Europea, a través de Expertise France, ha confirmado su apoyo a esta iniciativa, invitando a funcionarios gubernamentales de alto nivel de la Alianza Digital UE-ALC. La Red de CISO de LATAM está compuesta por líderes de opinión involucrados en el ciberespacio y el desarrollo de políticas digitales en la región de las Américas que entienden el valor de comprometerse de manera proactiva con los gobiernos, el sector privado, las organizaciones de la sociedad civil y las organizaciones internacionales para dar forma y avanzar en las prioridades comunes de ciberseguridad y política digital.

Desafíos de ciberseguridad en Costa Rica

En abril de 2022, Costa Rica fue objeto del quinto ciberataque más grande del mundo por parte del grupo de ransomware Conti, con sede en Rusia.[LXXIX] En concreto, Conti exigió 10 millones de dólares a cambio de no filtrar datos sensibles robados a la Secretaría de Hacienda, incluidos los registros fiscales de los ciudadanos.[LXXX] Conti encriptó y robó datos confidenciales, lo que provocó el cierre de sistemas críticos de declaración de impuestos y, a su vez, creó agitación económica.[LXXXI] El 31 de mayo de 2022, Costa Rica fue víctima de un segundo ataque en el que el grupo Hive aprovechó credenciales robadas para acceder a la Caja Costarricense de Seguro Social (CCSS), cerrando así los sistemas de la agencia.[LXXXII] Persistieron nuevos ataques, con otro hacker desactivando los sistemas médicos, lo que llevó a la cancelación de más de 158.000 procedimientos médicos.[LXXXIII] Todos los ataques exitosos se produjeron en centros de datos locales o en la nube privada. La recaudación de impuestos se vio gravemente afectada porque los sistemas en línea dedicados a esta tarea se vieron comprometidos. Muchas funciones gubernamentales, como el sistema médico público y los sistemas de recaudación de impuestos, volvieron a la documentación manual.[LXXXIV] Costa Rica nunca pagó el rescate exigido.[LXXXV] Si bien Conti se disolvió después de la invasión rusa de Ucrania, el país se convirtió en una lección de advertencia para la región. El grupo de ransomware pidió explícitamente el derrocamiento del gobierno costarricense, además de afirmar que esto debería servir como una advertencia para el resto del mundo. [LXXXVI]

Hasta junio de 2022, el gobierno costarricense ha gastado aproximadamente $24 millones en operaciones de respuesta, incluido dinero del fondo nacional de emergencia y recursos de la agencia.[LXXXVII] Alrededor de $4 millones fueron asignados por el fondo nacional de emergencia a varias agencias gubernamentales para la recuperación. Costa Rica se convirtió en la primera nación del mundo en declarar el estado de emergencia nacional debido a un ataque cibernético.[LXXXVIII] Solo la fase de rehabilitación le costó a la CCSS más de 18 millones de dólares de sus propios fondos, y no se utilizaron fondos de emergencia. Sin embargo, se informó de que la cantidad de dinero perdida debido al aplazamiento de las regulaciones de exportación e importación osciló entre 38 millones de dólares por día y 125 millones de dólares en 48 horas.[LXXXIX] La infraestructura no ha sido completamente reparada ocho meses después de la catástrofe, y miles de ciudadanos siguen sufriendo sus efectos.

En conclusión, a pesar de no pagar rescates, el gobierno y la infraestructura de Costa Rica quedaron inoperativos durante meses por los catastróficos ciberataques de 2022. Esta vulnerabilidad se vio exacerbada por la falta de una ley nacional de ciberseguridad, el progreso limitado en un proyecto de ley moderno de protección de datos y los recursos limitados de CSIRT. Según el Índice Global de Ciberseguridad (GCI) 2020 publicado por la UIT, la posición regional de Costa Rica se ha deteriorado de ocho a 18.[XC] Garantizar la resiliencia y la disuasión sigue siendo imperativo para evitar crisis similares.

Resultados de la entrevista

Esquiva preparación para la respuesta a incidentes cibernéticos

La principal conclusión de las entrevistas fue la brecha en la preparación para la respuesta, que fue destacada por todos los participantes. Esas deficiencias iban desde la falta de personal y de capacidad tecnológica hasta las deficiencias de comunicación entre las entidades de los sectores público y privado. Los entrevistados identificaron sistemáticamente la respuesta a incidentes cibernéticos como un área que necesita mejoras inmediatas en la planificación, los protocolos y los ejercicios de coordinación entre instituciones interdependientes. Para agravar estos problemas sistémicos de falta de preparación, los participantes enfatizaron repetidamente los déficits presupuestarios y de personal calificado que inhiben críticamente la movilización de recursos vitales necesaria para invertir en una ciberseguridad sólida y modernizada y una capacidad de mitigación rápida en las instituciones públicas y privadas. En general, la gravedad del ataque en 2022 provocó cambios, lo que dio lugar a un mandato para aumentar los equipos de respuesta, desarrollar protocolos y buscar asistencia internacional.

Impactos económicos en cadena

Los participantes compartieron que las repercusiones económicas del ataque de ransomware en 2022 afectaron a una amplia gama de sectores. La interrupción de los sistemas de pago administrados por el Ministerio de Hacienda, que afectó las transacciones financieras, las importaciones, las exportaciones y los servicios públicos, puso de relieve las consecuencias de gran alcance experimentadas por todos los entrevistados.

Reconocer la educación como piedra angular esencial

La mayoría de los entrevistados afirmaron que, a raíz del ataque, la ciberseguridad se había convertido en una prioridad para sus organizaciones y agencias a través de iniciativas que incluían el desarrollo de protocolos de incidentes, la actualización de la estrategia nacional y la exploración de alianzas externas. Sin embargo, si bien es necesario fortalecer la gobernanza y las capacidades, los participantes también citaron la falta de higiene cibernética y conciencia de las amenazas entre los usuarios finales (personas que realmente usan un producto en particular) como factores que con frecuencia exacerban el éxito de los incidentes y las dificultades de contención. Como tal, las campañas de concientización y el cultivo de la cultura de la ciberseguridad pueden integrar una capa humana importante en la defensa cibernética.

Perspectivas sobre la adopción de la nube para disminuir el riesgo de ciberseguridad

Los entrevistados mencionaron que numerosas agencias gubernamentales ya han adoptado servicios en la nube y han reconocido su valor en la mitigación de riesgos. Si bien los entrevistados reconocieron beneficios potenciales, como la mejora del acceso y el rendimiento, algunos

todavía tenían preocupaciones sobre los costos y los posibles riesgos de seguridad asociados, sin especificar si las preocupaciones estaban relacionadas con los servicios de nube pública o privada.

Evolución de los marcos de ciberseguridad centrados en el NIST

Los entrevistados expresaron su esperanza de que los RMF existentes, como el Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST CSF), puedan adoptarse en ausencia de regulaciones nacionales maduras. A finales de 2023, la embajada de EE. UU. llevó a cabo iniciativas conjuntas de capacitación en ciberseguridad con funcionarios costarricenses que se centraron en el CSF del NIST e involucraron a personal de TI y ciberseguridad de todo el gobierno costarricense. Estas sesiones de capacitación cooperativa demuestran que Costa Rica está investigando activamente la adopción de un RMF como un elemento crucial de desarrollo de capacidades que supere las capacitaciones.

Los ataques de ransomware pusieron de manifiesto las brechas de preparación que enfrenta Costa Rica y alentaron al país a invertir en la construcción de infraestructura vital. Este aumento en la inversión ha propiciado un cambio importante en el liderazgo de la preparación de seguridad cibernética de Costa Rica y el desarrollo de procedimientos exhaustivos.

Análisis comparativo entre Costa Rica y Colombia

Las respuestas al ransomware en Costa Rica y Colombia revelaron importantes deficiencias internas en las áreas de evaluación de impacto, comunicación y detección. La escasez crónica de fondos y experiencia obstaculiza las iniciativas de mejora de maneras únicas. Mientras Colombia busca mejorar las capacidades de rastreo de incidentes, Costa Rica sufre de deficiencias de recursos que frustran las operaciones existentes del CSIRT y la coordinación de la contención. Ambos países reconocen la insuficiente preparación técnica y la necesidad de aumentar la fuerza laboral de ciberseguridad.

En consecuencia, Colombia buscó el desarrollo de capacidades internas, particularmente en torno a la inteligencia de amenazas. Costa Rica, sin embargo, se centró más en las alianzas internacionales para elevar las capacidades de respuesta en dimensiones como la medicina forense y la capacitación de la fuerza laboral. En cuanto a la implementación de la RMF, ambos países están desarrollando estrategias de gobernanza cibernética centradas en la adopción selectiva de marcos NIST como estándar global, aunque Costa Rica ha emprendido iniciativas de capacitación más tangibles hasta el momento.

Por último, ambos países reconocen la importancia de la evolución estratégica, pero han adoptado enfoques diferentes para su implementación. Si bien en el pasado han dependido de la asistencia de aliados extranjeros para fortalecer la preparación para la respuesta cibernética, Colombia y Costa Rica reconocen que prepararse para más amenazas cibernéticas es la forma más segura de avanzar.

CASO DE ESTUDIO:

CHILE

Introducción

Los ataques a empresas privadas o agencias gubernamentales pueden afectar el entorno económico y social de cualquier país, especialmente de una nación en desarrollo como Chile. Comprender los desafíos, la infraestructura y los recursos específicos de un país es fundamental para desarrollar una estrategia para mitigar el impacto de futuros incidentes de ciberseguridad. Esta sección estudia el panorama de la ciberseguridad en Chile, incluyendo su historia y las preocupaciones y desafíos actuales.

Panorama de la Política de Ciberseguridad en Chile

A partir de principios de la década de 2000, Chile aprobó múltiples leyes que regulan la seguridad de las comunicaciones electrónicas dentro del gobierno. Sin embargo, no fue hasta 2015 que Chile aprobó el Decreto 533, que creó un Comité Interministerial de Ciberseguridad para asesorar sobre política y coordinación nacional de ciberseguridad.[XCI] Este decreto definió la ciberseguridad, delineó las funciones del comité y ordenó la creación de una comisión técnica asesora.[XCII] El comité estaba integrado por representantes de los organismos gubernamentales pertinentes y se reunía periódicamente para proponer protocolos de coordinación y proporcionar asesoramiento técnico. A través de este comité, Chile se aseguró de liderar los esfuerzos de ciberseguridad a nivel nacional en lugar de desarrollarla a través de actores privados.

En 2017, Chile presentó su primera Política Nacional de Ciberseguridad 2017-2022.[XCIII] La política presentó dos políticas sobre la implementación de objetivos de largo plazo para que Chile logre un ciberespacio más seguro. Los objetivos específicos incluyeron el desarrollo de una infraestructura de información robusta para resistir y recuperarse de incidentes cibernéticos, desarrollar una industria nacional de ciberseguridad y participar en foros internacionales.[XCIV] En 2018, el Congreso aprobó una ley que establecía octubre como el Mes de la Ciberseguridad del país, que tenía como objetivo crear conciencia y educación pública sobre el tema, lo que indica un cambio por parte del gobierno de Chile hacia la priorización de la ciberseguridad. [XCV]

En 2019, el Departamento del Interior y Seguridad Pública proclamó una resolución que establecía una subdivisión llamada Unidad de Coordinación de Ciberseguridad.[XCVI] Luego, el departamento amplió y actualizó la unidad en 2023.[XCVII] El propósito de esta unidad era llevar a cabo las recomendaciones de ciberseguridad del presidente para políticas, leyes y regulaciones.[XCVIII] Estas recomendaciones incluían las mejores prácticas, protocolos e infraestructuras ideales, una mayor coordinación entre sectores y capacitación.[XCIX] A través de esta nueva unidad, se creó el CSIRT.[C] Este equipo tiene la tarea de coordinar la respuesta a incidentes dentro del país y apoyar a diferentes departamentos gubernamentales con incidentes que puedan afectar sus operaciones. [CI]

Chile continúa desarrollando estándares y metas para su ciberseguridad y la infraestructura relacionada, especialmente con la aprobación de la Agenda Digital Chile 2035 en 2022. Esta estrategia digital tiene como objetivo digitalizar el 95% de los servicios públicos en 2025 y el 100% en 2035.[CII] El enfoque explícito de la estrategia en ciberseguridad esboza cinco objetivos: (1) establecer un ecosistema dinámico de ciberseguridad, (2) crear un marco institucional para difundir la ciberseguridad entre la población, (3) mejorar los programas de capacitación y educación en ciberseguridad de alta calidad, (4) abordar la

legislación vigente en materia de ciberseguridad y (5) garantizar la existencia de mecanismos que permitan la cooperación entre fronteras. Reconociendo la importancia crítica de la ciberseguridad, Chile está priorizando los esfuerzos de colaboración entre los sectores privado, académico, gubernamental e internacional para gestionar estos desafíos de manera efectiva.

El 4 de diciembre de 2023 entró en vigor la Política Nacional de Ciberseguridad 2023-2028.[CIII] Entendiendo que la tecnología cambia rápidamente, Chile ha puesto en vigencia esta Política solo durante el período 2023-2028.[CIV] Además, esta política fomentó la aprobación de la Ley Marco de Ciberseguridad para combatir aún más los problemas de seguridad. El Congreso chileno aprobó el proyecto de ley, que creará una nueva agencia de ciberseguridad: la Agencia Nacional de Ciberseguridad (ANCI).[CV] Este proyecto de ley fue aprobado por el Tribunal Constitucional y publicado en el Diario Oficial. Ramón Molina, director ejecutivo del Centro de Innovación UC y copresidente de la iniciativa, dijo que "la ley también destacó que la dependencia podrá multar a los infractores de las normas de ciberseguridad, donde las sanciones se categorizan como leves, oscilando entre 0 a 5000 UTM para Servicios Esenciales (SE)".[CVI] En Chile, los servicios esenciales abarcan los prestados por la administración, el Coordinador Eléctrico Nacional y las concesiones de servicio público. Otros servicios esenciales pueden incluir la generación de electricidad; el transporte de combustibles; el suministro de agua potable; telecomunicaciones, infraestructura digital y tecnologías de la información gestionadas por terceros; transporte aéreo, ferroviario o marítimo; servicios financieros; servicios de salud; y productos farmacéuticos. [CVII]

Además de la creación de la ANCI, la ley también creará el CSIRT Nacional, el CSIRT de Defensa Nacional, el Consejo Multisectorial de Ciberseguridad y la Red Estatal de Conectividad Segura. Según lo descrito por la ministra de Interior y Seguridad Pública, Carolina Tohá, esta nueva ley definirá estándares para los prestadores de servicios esenciales con la ayuda de instituciones específicamente diseñadas y certificadas para validarlos.[CVIII] Además, la ley proporcionará educación y talleres para los trabajadores, ejercicios teóricos, simulaciones y análisis de las redes, y sistemas de información y detección.[CIX] Estas instituciones tendrán el deber activo de reportar cualquier incidente o incumplimiento al CSIRT. Además, la nueva ley permitirá la creación de diferentes CSIRT[CX] sectoriales para gestionar la ciberseguridad de las industrias correspondientes, como el nuevo CSIRT de defensa.

El propósito de la ANCI es mejorar y ampliar el trabajo del CSIRT a través de la consolidación de tareas y el aumento de los recursos. La agencia asesorará al presidente de Chile sobre la política nacional de ciberseguridad y cualquier programa relacionado.[CXII] Las disposiciones clave incluyen obligaciones específicas de presentación de informes, multas por incumplimiento, mandatos para que las empresas privadas aborden los incidentes y una mayor coordinación entre los sectores público y privado.[CXIII] Además, creará una categoría especial de operadores de vital

importancia para los proveedores de servicios esenciales que dependen de las redes y sistemas de información.[CXIV] La ley, a través de la ANCI y otros actores, exigirá funciones especiales a estos operadores, como sistemas de seguridad, capacitación y análisis constante.[CXV] Al establecer los estándares para los servicios y operadores esenciales, la agencia garantizaría la protección de los activos digitales y la información de los ciudadanos.[CXVI] En general, la ley tiene como objetivo fortalecer la postura de ciberseguridad de Chile y posicionar al país como líder en la región.

Participación y contribuciones del sector privado

Como se ha descrito anteriormente, el proyecto de ley se aplicará a las empresas del sector privado que presten servicios esenciales. El sector privado está muy involucrado en el desarrollo y aplicación de diferentes medidas de ciberseguridad. Muchas organizaciones privadas han surgido para abordar las preocupaciones de ciberseguridad de empresas privadas, sectores específicos y otras industrias. Una de estas organizaciones es la Alianza Chilena de Ciberseguridad, que fue fundada por nueve instituciones que representan a importantes industrias de Chile, como el transporte y la defensa. Esta organización incluye esfuerzos colaborativos de diferentes organizaciones gubernamentales, privadas y educativas.[CXVII] Otra organización es el Instituto Nacional de Ciberseguridad de Chile, que educa y crea conciencia sobre la seguridad de la información para aumentar la confianza social de individuos y empresas.[CXVIII] Del mismo modo, el surgimiento de asociaciones gremiales con enfoque regional ha buscado fortalecer el desarrollo de la industria tecnológica en Chile. Un ejemplo de una de estas asociaciones es Chiletec, un grupo de más de 100 empresas chilenas del sector tecnológico. [CXIX]

Colaboraciones Internacionales

Chile es signatario de la Convención de Budapest, que es "un marco que permite a cientos de profesionales de las Partes compartir experiencias y crear relaciones que faciliten la cooperación en casos específicos, incluso en emergencias, más allá de las disposiciones específicas previstas en esta Convención".[CXX] A través de estas convenciones, Chile busca alinear sus esfuerzos con las normas, estándares y mejores prácticas internacionales y aceptar universalmente la definición de delito cibernético.

Además, Chile está tratando de encabezar el movimiento de ciberseguridad en América Latina al albergar la participación internacional de las partes interesadas. El 9º Congreso Latinoamericano Tecnología y Negocios América Digital 2024 tendrá lugar en Santiago en abril, donde se espera que más de 5000 profesionales de la alta dirección asistan a sesiones sobre tecnología y negocios.[CXXI]

Desafíos de ciberseguridad en Chile

La creciente digitalización de Chile presentará riesgos de ciberseguridad si los servicios y estructuras no están debidamente protegidos y no se prioriza la

respuesta a incidentes. Además de las graves consecuencias sufridas por el ataque a la red IFX en Colombia, Chile también ha experimentado importantes ciberataques en los últimos años.[CXXII] Por ejemplo, en mayo de 2023, el Ejército de Chile sufrió un ciberataque por parte de un grupo de ransomware llamado Rhysida, que afectó las redes internas del Ejército y provocó una violación de datos.[CXXIII] Durante los ataques, los sitios web del ejército no estaban disponibles de forma intermitente, y Rhysida publicó el 30% de los datos robados en su sitio de filtración después del ataque.[CXXIV] La causa raíz de este ataque aún no está clara, pero se realizó un arresto contra un miembro del ejército por su presunta participación en el ataque.[CXXV] Del mismo modo, en octubre de 2023, el grupo de ransomware Black Basta infectó parte de la infraestructura digital del Servicio Nacional de Aduanas de Chile.[CXXVI] El CSIRT del Ministerio del Interior y Seguridad Pública emitió una advertencia al detectar la infección, pero precisó que el incidente ocurrió en una parte limitada de la infraestructura digital.[CXXVII] A pesar de la desconexión de la red, se garantizó que el incidente no interrumpiera las operaciones de la aduana y se tomaron medidas preventivas para evitar infracciones.[CXXVIII]

Otro desafío de ciberseguridad en Chile es la escasez de trabajadores especializados en la industria de TI. El Servicio Nacional de Capacitación y Empleo (SENCE) pronosticó que a mediados de 2022 habría un déficit anual de alrededor de 6.000 profesionales de TI en Chile.[CXXIX] Según un estudio realizado por la Fundación País Digital y Accenture, Chile podría perder cerca de $13.000 millones en crecimiento para 2030 si la población chilena no está preparada para las habilidades de mercado necesarias en el sector.[CXXX]

En general, la arquitectura y la infraestructura de ciberseguridad de Chile han mejorado mucho en los últimos años. Chile demuestra un compromiso con la gestión integral de los riesgos cibernéticos, como lo demuestra la creación del Comité Interministerial de Ciberseguridad y la aprobación de leyes como la Ley Nacional de Ciberseguridad. La resiliencia de la ciberseguridad se ha mejorado aún más mediante la cooperación con socios internacionales y el sector comercial. Sin embargo, problemas como la falta de trabajadores de TI calificados y las amenazas cibernéticas persistentes enfatizan la importancia de la atención continua a los detalles y el apoyo financiero para las iniciativas de ciberseguridad.

Postura de ciberseguridad de Chile

Los entrevistados compartieron que algunas leyes existentes tienen lagunas relacionadas con los mecanismos de aplicación, aunque comparten el optimismo de que la Ley Marco de Ciberseguridad e Infraestructuras Críticas combata algunos de estos problemas. Los entrevistados creen que se han realizado esfuerzos para cambiar las regulaciones hacia principios flexibles en lugar de tecnologías específicas, dada la rápida tasa de cambio en la industria.

Muchos entrevistados también observaron una falta de eficiencia en el marco jurídico existente, pero a su vez, una sensación de optimismo por las leyes que están en proceso de aprobación. La Ley Marco de Ciberseguridad e Infraestructuras Críticas proporcionará un marco más actualizado y la creación de una nueva agencia federal de ciberseguridad. Sin embargo, los expertos siguen preocupados por el hecho de que un organismo de ese tamaño y alcance necesite más recursos de los que se otorgan actualmente para lograr sus objetivos.

Perspectivas sobre las tendencias regionales

Chile comparte la estrategia reactiva que se observa en toda América Latina: experimentar ataques, responder en consecuencia y mejorar la resiliencia después en lugar de emprender una prevención proactiva. Al igual que otros países de la región, la apresurada digitalización pandémica de Chile exacerbó las brechas de seguridad en una sociedad más interconectada. Estas brechas fueron abordadas por una sólida ley de ciberseguridad aprobada en diciembre de 2023.

Evolución de los marcos de ciberseguridad centrados en el NIST

Los entrevistados expresaron que Chile valora los RMF como mejores prácticas de referencia, pero enfatizaron que estos marcos requieren localización. Con diferentes modelos operacionales y sistemas jurídicos, los enfoques de talla única no pueden abordar las cuestiones relativas a las políticas y las amenazas específicas de cada país. No obstante, los marcos globales pueden informar los esfuerzos de Chile para desarrollar regulaciones ágiles centradas en principios duraderos en lugar de tecnologías temporales.

Perspectivas sobre la adopción de la nube para disminuir los riesgos de ciberseguridad

En 2023, el gobierno chileno publicó una guía [CXXXI] para el uso de servicios en la nube en el sector público. Esta guía tiene como objetivo proporcionar definiciones, directrices y mejores prácticas uniformes para los organismos públicos que utilizan servicios en la nube en el marco de un enfoque "inteligente en la nube". Este enfoque recomienda a los organismos públicos que adopten soluciones de nube pública cuando sean adecuadas para sus objetivos, proporcionen una protección de datos adecuada y ofrezcan valor financiero.

CASO DE ESTUDIO:

PANAMÁ

Introducción

Esta revisión de la literatura enfatiza el compromiso de Panamá con la creación de una infraestructura de ciberseguridad sólida y flexible. Examina el enfoque distintivo de Panamá para proteger la seguridad nacional, los intereses económicos y los derechos de sus ciudadanos en un mundo que depende cada vez más de la tecnología digital. Esta revisión sienta las bases para un análisis en profundidad de los métodos, obstáculos y avances de Panamá en el campo de la ciberseguridad.

Visión general de la política de ciberseguridad en Panamá

Durante la última década, Panamá ha enfatizado la protección de los servicios esenciales con su "estrategia enfocada en generar confianza en el uso del ciberespacio para obtener beneficios de conectividad con el mínimo riesgo".[CXXXII] A partir de 2011, Panamá estableció una estrategia nacional integral de ciberseguridad, siendo un esfuerzo notable la creación de un CSIRT.[CXXXIII] Este equipo se encargó de abordar los incidentes de ciberseguridad que afectan tanto al sector público como al privado.[CXXXIV] En 2013, Panamá también estableció seis pilares de su estrategia de ciberseguridad: (1) proteger la privacidad y los derechos humanos, (2) prevenir y sancionar el delito cibernético, (3) fortalecer la infraestructura crítica nacional, (4) construir una base industrial nacional de ciberseguridad, (5) desarrollar una cultura de ciberseguridad y (6) mejorar la seguridad y la capacidad de respuesta de las entidades públicas.[CXXXV] En consonancia con estos seis pilares, el CSIRT señala que entre sus objetivos se encuentra la "prevención, tratamiento, identificación y resolución de ataques a incidentes de seguridad en los sistemas informáticos que conforman la infraestructura crítica del país y el acceso a la información de los ciudadanos panameños".[CXXXVI] Además de cumplir con estos objetivos, CSIRT Panamá también es responsable de aumentar la comprensión general de la nación sobre la ciberseguridad no solo para crear conciencia y alfabetización digital, sino también para combatir activamente las amenazas cibernéticas y la interrupción del servicio en línea.[CXXXVII]

En marzo de 2019, Panamá promulgó el Decreto 285/2021, que regula las leyes de privacidad y protección de datos en el país. Esta ley obliga a los encargados del tratamiento a obtener el consentimiento previo de los interesados y a ser debidamente informados del uso propuesto de sus datos personales. La Asamblea Nacional de Panamá aprobó el Decreto Ejecutivo 285/2021 de la Ley de Protección de Datos Personales, que regula los principios, derechos, obligaciones y procedimientos en materia de protección de datos personales.[CXXXVIII] Esta ley fue creada con el propósito de proteger los datos de los panameños. Una disposición adicional a esta ley incluso prevé una compensación a los panameños por el uso indebido de sus datos. En 2020, la Autoridad Nacional para la Innovación Gubernamental (AIG) de Panamá anunció la nueva "Agenda Digital Nacional 2022-2023" como un instrumento estratégico para promover la reactivación económica, involucrando a las entidades en los procesos de mejora y aumentando la innovación y la colaboración entre los sectores público y privado. [CXXXIX] Sobre estas bases, se promulgó la Resolución 17/2021, que describe la Estrategia Nacional de Ciberseguridad para el período 2021-2024.[CXL] Esta estrategia hace hincapié en varias áreas críticas, incluida la prevención y prohibición de comportamientos delictivos en el ciberespacio, el fomento de la innovación y la capacitación en ciberseguridad y la protección de la privacidad de la información personal.

La infraestructura actual de ciberseguridad depende en gran medida del éxito de la Agenda Digital Nacional de Panamá. A través de una mayor colaboración, Panamá pidió que cada sector cree su propia agenda digital alineada con la nueva Agenda Digital Nacional 2022-2023 y apunte a lograr otros objetivos, como definir estándares y condiciones para el uso de las TIC, especialmente la nube y el 5G.[CXLI] Sin embargo, el país enfrenta varios desafíos para implementar con éxito la agenda 2022. Algunos de estos desafíos incluyen la dificultad para "asegurar la infraestructura y los servicios críticos, impulsar la inversión privada en el ecosistema digital y fortalecer las plataformas de interoperabilidad nacionales y sectoriales". [CXLII]

Durante la última década, Panamá ha promulgado leyes y estrategias fundamentales de ciberseguridad que priorizan el crecimiento confiable del ecosistema digital a través de equipos de respuesta a incidentes, salvaguardas de datos/privacidad y disuasión del delito cibernético. Sin embargo, la Agenda Digital Nacional de Panamá, destinada a estimular la innovación y la actividad económica, se ha enfrentado a preocupantes obstáculos de implementación en torno a la entrega de una sólida seguridad de infraestructura crítica y tecnologías integradas. Con ambiciosos plazos de transformación desafiados por persistentes brechas de capacidad, el compromiso sostenido de gobernanza junto con las asociaciones público-privadas sigue siendo esencial para que Panamá haga realidad su visión de resiliencia cibernética.

Colaboraciones internacionales y participación del sector privado

También se han reforzado los marcos jurídicos para combatir la ciberdelincuencia. La Ley 79 de 2013 llevó a la adopción por parte de Panamá de la Convención de Budapest. El Código Penal panameño, en particular los artículos 289 a 292, tipifica específicamente diversas formas de conducta indebida cibernética, como el acceso no autorizado, la interferencia y el uso indebido de datos, mediante la imposición de sanciones por estos delitos.[CXLIII] Además, Panamá ha estado buscando activamente asociaciones de ciberseguridad en todo el mundo, firmando tratados de cooperación con países como Israel, España y Costa Rica. De cara al futuro, Panamá tiene como objetivo aumentar aún más la capacitación, el desarrollo de capacidades y la coordinación a través de la colaboración internacional. Los esfuerzos recientes incluyen la incorporación a los equipos de respuesta a incidentes de la OEA y Global FIRST, así como la firma de un acuerdo de trabajo con Eurojust "para permitir una cooperación estructurada y más estrecha en la lucha contra el crimen organizado". [CXLIV] Por último, como se menciona en la revisión bibliográfica de Costa Rica, Panamá ha formalizado acuerdos cibernéticos con la República Dominicana y Costa Rica.[CXLV]

Desafíos de ciberseguridad en Panamá

En Panamá debido a la pandemia, la necesidad de servicios y software de ciberseguridad en los sectores público y privado ha crecido significativamente en los últimos dos años, en los que se registró un aumento del 421% en delitos y ataques cibernéticos.[CXLVI] La mayoría de los casos ocurrieron en 2021 con 794 denuncias, el 68% de las cuales fueron fraudes, mientras que los casos de extorsión sumaron 423 a finales de 2020. Según los expertos en ciberseguridad, las empresas estadounidenses han dominado el sector de la ciberseguridad con aproximadamente el 60% del mercado total.[CXLVII]

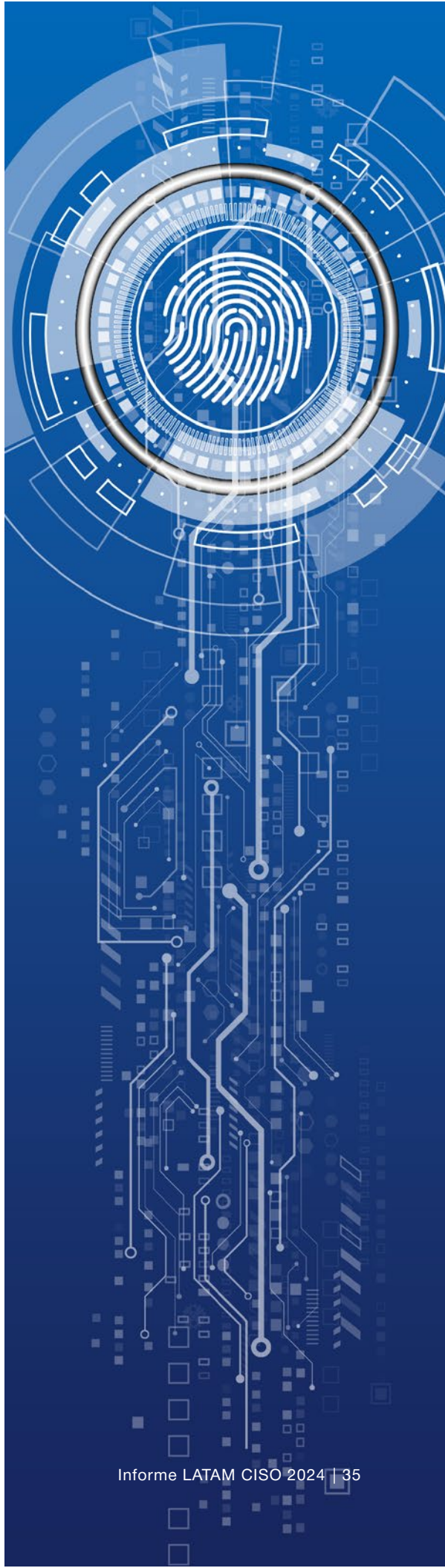
El Índice AML de Basilea es una herramienta anual de clasificación y análisis de riesgos centrada en evaluar las vulnerabilidades del blanqueo de capitales y la financiación del terrorismo a nivel nacional. Se basa en 18 fuentes acreditadas, entre ellas el Grupo de Acción Financiera Internacional (GAFI), Transparencia Internacional y el Banco Mundial. En 2023, "Panamá obtuvo una puntuación alta en este índice, lo que lo convierte en el más susceptible a las amenazas cibernéticas".[CXLVIII] En concreto, Panamá registró una puntuación de alto riesgo en el Índice de Prevención de Blanqueo de Capitales (AML) de Basilea de 2023, según el análisis del Informe Global de Ciberdelincuencia de Fortra.[CXLIX] A pesar de que Panamá ha promulgado leyes contra los delitos financieros, se destaca la deficiente aplicación de la ley como un factor que perpetúa las debilidades sistemáticas que permiten las amenazas de lavado de dinero y financiamiento del terrorismo. Según el mismo informe, Panamá fue el país con el puntaje más bajo en desarrollo digital, que se basa en su desarrollo de TIC y preparación para la red.[CLI] Si bien Panamá está progresando diligentemente hacia la resolución de sus desafíos existentes, la nación aún enfrenta un viaje considerable en su ambición de emerger como un centro tecnológico competitivo a nivel mundial.

Preocupaciones regulatorias

El papel de Panamá como centro de comunicaciones sofisticadas de fibra óptica y su condición de centro financiero con numerosos bancos internacionales requieren un régimen robusto de ciberseguridad. La introducción de la Ley 159 de 2020, que tiene como objetivo establecer centros logísticos para la fabricación y el reempaque, subraya aún más la necesidad de estrictas protecciones cibernéticas. El BID enfatiza que una estrategia integral, que equilibre las necesidades de seguridad con el crecimiento económico y respete los derechos a la libertad de expresión y privacidad, es crucial para una ciberseguridad sostenible. El compromiso de Panamá con la protección de la infraestructura crítica, la adopción de marcos de mejores prácticas y la garantía de la privacidad y confidencialidad de los datos es cada vez más imperativo para su continuo avance en la era digital. [CLII]

Impactos socioeconómicos de las brechas de ciberseguridad

El Informe Global de Ciberdelincuencia 2023 indica que Panamá es el país con mayor riesgo de ciberdelincuencia, lavado de activos y financiamiento del terrorismo, con un Índice AML de Basilea de 5.81/10.[CLIII] Esta posición se determinó calculando un 5,81 para el Índice AML de Basilea. La ciberseguridad de Panamá obtuvo sistemáticamente una mala puntuación, con el peor nivel de desarrollo digital y el Índice AML de Basilea.[CLIV] El lavado de dinero ha afectado en particular a las operaciones comerciales panameñas, "con un estimado de $935 mil millones que se lavan anualmente. A pesar de contar con leyes para abordar el lavado de dinero, las autoridades rara vez las aplican".[CLV] Esta falta de implementación ha exacerbado la ciberdelincuencia, especialmente el lavado de dinero realizado en línea. Si esta falta de aplicación continúa, puede afectar a Panamá a través de la disminución de la inversión económica extranjera y la confianza social.



Perspectivas de Panamá sobre la respuesta de Colombia al ransomware

Los participantes señalaron que cuando el ransomware golpeó por primera vez la región, Colombia compartió advertencias de amenazas para ayudar a las entidades de mayor riesgo de Panamá. Panamá observó de cerca las comunicaciones públicas de Colombia durante la respuesta al incidente. Este intercambio de información permitió minimizar el temor en el país, dada la estrecha relación de Panamá con Colombia. Después del incidente, Colombia colaboró con los CSIRT regionales, lo que brindó a Panamá la oportunidad de aprender de su experiencia. En el caso de Panamá, la experiencia de Colombia puso de relieve la necesidad de implementar leyes obligatorias de notificación de incidentes cibernéticos a nivel nacional.

Perspectivas sobre la adopción de la nube para disminuir los riesgos de ciberseguridad

Aunque actualmente está restringido por las recientes leyes de soberanía de datos, Panamá está abierto a posibles colaboraciones con proveedores para establecer soluciones locales en la nube. Estas soluciones tendrían como objetivo aprovechar las eficiencias de la digitalización y, al mismo tiempo, mantener el control nacional sobre los sistemas críticos y el almacenamiento de datos. En 2024, la AIG de Panamá publicó la Resolución 52, que establece lineamientos para la ubicación de bases de datos que operan bajo el concepto de computación en la nube o servicios en la nube. Este enfoque subraya el reconocimiento de los beneficios de la nube al tiempo que aborda las preocupaciones percibidas.

Evolución de los marcos de ciberseguridad centrados en el NIST

Los participantes compartieron que Panamá sigue enfoques como el CSF del NIST, los requisitos del RGPD de la UE y los controles de seguridad ISO como referencias, al tiempo que adapta las políticas y regulaciones a su entorno de riesgo único y a las limitaciones existentes en el inventario de software. Esta localización personalizada de las mejores prácticas globales establecidas, combinada con la flexibilidad de las agencias gubernamentales, permite a Panamá cubrir los rápidos cambios tecnológicos dentro de su gobernanza cibernética.

En conclusión, Panamá busca avanzar de manera constante hacia la madurez cibernética a través de la colaboración global y la adopción personalizada de nuevos estándares y tecnologías de ciberseguridad. La nación reconoce la importancia crítica de las defensas cibernéticas sólidas y la resiliencia en la era digital actual. Sin embargo, Panamá entiende que es poco probable que un enfoque único para todos tenga éxito y, en cambio, está siguiendo una estrategia pragmática y metódica. Esto implica capitalizar las experiencias de otros países de la región que se encuentran más avanzados en la curva de madurez cibernética, al tiempo que evalúa

cuidadosamente su propio panorama de riesgos, infraestructura, recursos y fuerza laboral cibernética únicos para adaptar las soluciones a sus requisitos específicos. Al aprender de otros a través de asociaciones estratégicas e intercambio de conocimientos, pero realizando implementaciones calibradas y personalizadas para su entorno, Panamá tiene como objetivo reducir continuamente los riesgos y mejorar las capacidades a lo largo del tiempo, salvaguardando sus sistemas críticos y activos de datos. En última instancia, este enfoque equilibrado permite a Panamá mejorar su preparación cibernética de una manera acorde con sus aspiraciones socioeconómicas, logrando una postura cibernética resiliente y segura para la era digital.

Conclusiones de la entrevista

A partir de entrevistas realizadas en Colombia, Costa Rica, Panamá y Chile, a continuación, se resumen los principales hallazgos y tendencias relacionados con las actitudes de ciberseguridad y la preparación para la respuesta al ransomware:

- Reconocimiento general del aumento de los riesgos de ransomware y los requisitos de seguridad de datos críticos para las organizaciones del sector público y comercial.
- Persisten brechas sustanciales en torno a la preparación para incidentes cibernéticos, los protocolos de respuesta, la coordinación, la dotación de personal y las capacidades técnicas.
- Los déficits presupuestarios y de capacitación limitan las inversiones en seguridad y la movilización de una respuesta rápida.
- Comprender la necesidad de aumentar las prioridades de gobernanza y el desarrollo de capacidades debido a las amenazas cibernéticas.
- Adoptar el desarrollo de la fuerza laboral cibernética como un componente fundamental de la conciencia y la cultura.
- Habilitación de políticas de seguridad flexibles mediante la personalización local de marcos globales.
- Consenso sobre el riesgo y los beneficios de la ciberseguridad de la adopción de servicios de nube pública y la necesidad de abordar las preocupaciones percibidas sobre el control de datos.

En última instancia, las entrevistas indicaron desafíos comunes de respuesta al ransomware y oportunidades para el crecimiento colectivo a través del desarrollo de la fuerza laboral y el aumento de la capacidad, incluso cuando las perspectivas cibernéticas variaban en algunas áreas. Estos conocimientos abren nuevas posibilidades para el avance coordinado de la seguridad.

Resultados de la encuesta

Para comprender mejor el panorama de la ciberseguridad en América Latina, se encuestó a más de 150 CISO y otros profesionales de alto nivel de la región. El objetivo de la encuesta fue obtener una visión general de lo que piensan los profesionales de la ciberseguridad en la región sobre temas como los RMF, el uso de infraestructura de ciberseguridad basada en la nube pública para mitigar el riesgo, y más. Los encuestados trabajaban en los sectores público y privado y procedían de diversos países. Los encuestados procedían de Colombia (19%), Argentina (14%), Costa Rica (13%), Chile (8%), Guatemala (6%) y Bolivia (5%), así como de Brasil, Cuba, Ecuador, El Salvador, Haití, Honduras, México, Nicaragua, Panamá, Perú, República Dominicana y Uruguay. La mayoría de los encuestados trabaja en el sector privado (67%) o en el sector público (27%), y otros representan a la sociedad civil (2%) y al mundo académico (3%).

Un tema común en esta investigación es la necesidad de invertir en la fuerza laboral y la capacitación en ciberseguridad. De los que respondieron a la encuesta, el 84% eran hombres. Esto pone de relieve la necesidad de, dentro de un régimen integral de formación de la mano de obra, una mayor diversidad en la mano de obra de ciberseguridad. Aumentar el acceso a la tecnología y la ciberseguridad para las mujeres y las minorías debería ser una prioridad para todos los países.
El análisis de la encuesta se divide en dos categorías clave: 1) Marcos de gestión de riesgos (RMF) y 2) el uso de infraestructura de ciberseguridad basada en la nube pública. La sección RMF examina la adopción de varios modelos de marco de gestión de riesgos, como NIST e ISO, en diferentes industrias y tamaños de organizaciones. Explora la efectividad percibida, los desafíos y los beneficios de emplear RMF para la evaluación y mitigación de riesgos. La sección de seguridad en la nube se centra en la tendencia de aprovechar las soluciones de ciberseguridad basadas en la nube pública, como SIEM, gestión de vulnerabilidades e IAM. Investiga el alcance de la adopción de la seguridad en la nube, los impulsores como la escalabilidad y el acceso a la tecnología de vanguardia, así como las preocupaciones en torno a la seguridad en la nube, la privacidad de los datos y el cumplimiento. Esta descripción general proporciona una hoja de ruta para comprender el estado de la implementación de RMF y el uso de infraestructuras de ciberseguridad basadas en la nube pública según los resultados de la encuesta.

Marco de Gestión de Riesgos
(RMF)

Pregunta 9: En una escala de 5 puntos de muy de acuerdo a totalmente en desacuerdo, ¿cómo calificaría su creencia de que la implementación de un RMF puede mejorar los esfuerzos de su organización/agencia gubernamental contra las amenazas cibernéticas como el ransomware?

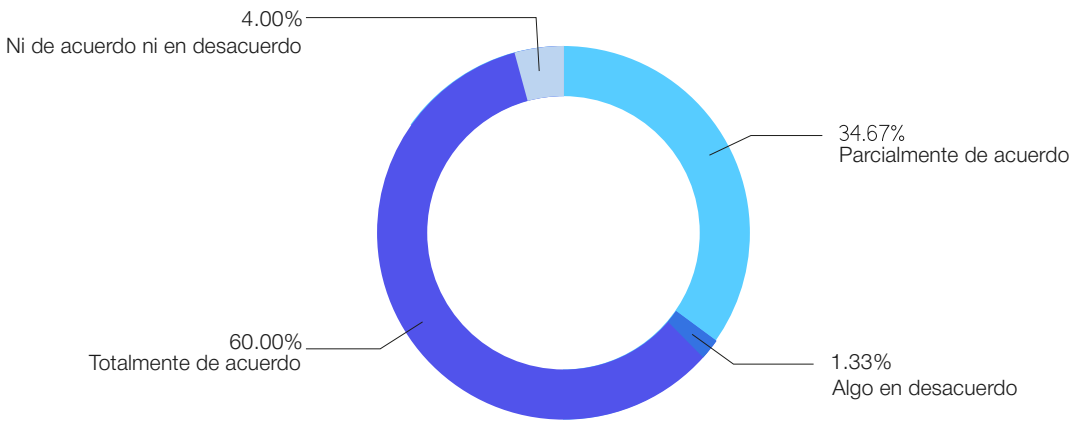


Figure 1: RMF Capacidades

Pregunta 7: Describa lo que considera más valioso en un marco de ciberseguridad.

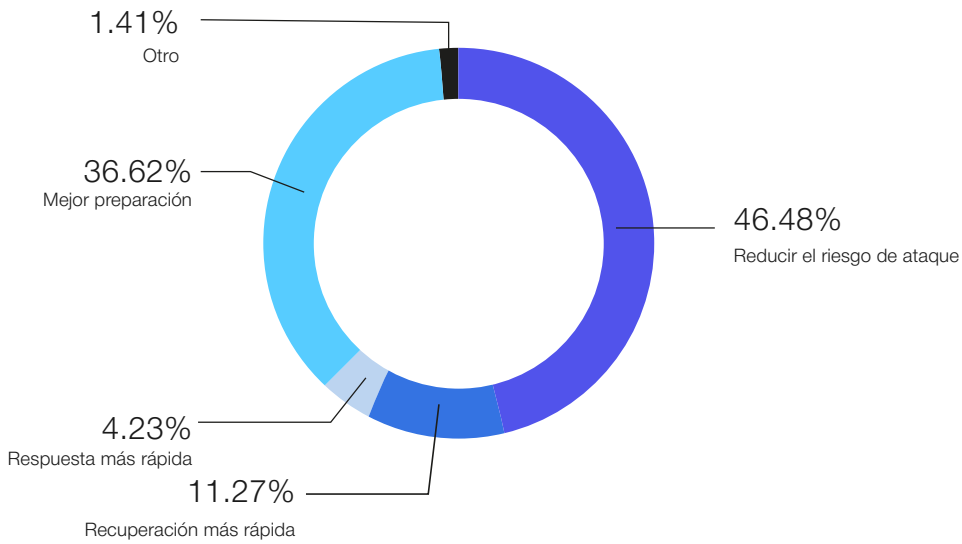


Figure 2: Valor del marco de ciberseguridad

Pregunta 8: ¿Emplea actualmente alguno de los siguientes marcos?

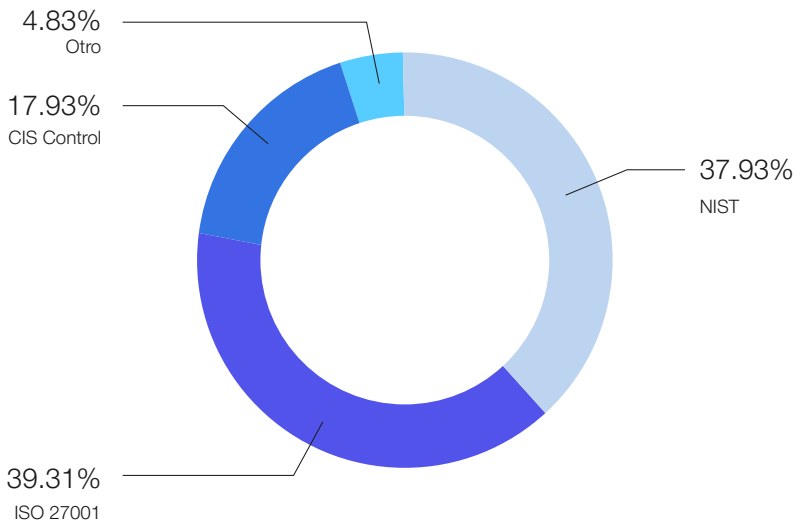


Figure 3: Marcos utilizados

Pregunta 10: ¿Ha implementado un RMF en la estrategia de ciberseguridad de su organización/empresa/agencia gubernamental?

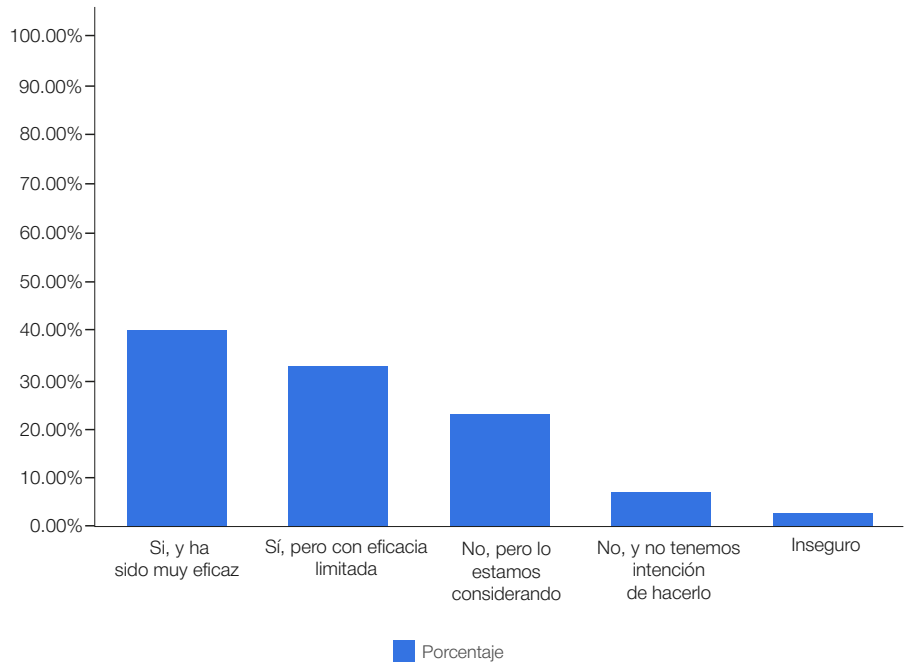


Figure 4: RMF Implementación y eficacia

Pregunta 11a: ¿Qué desafíos, si los hay, ha encontrado al considerar la creación de un RMF?

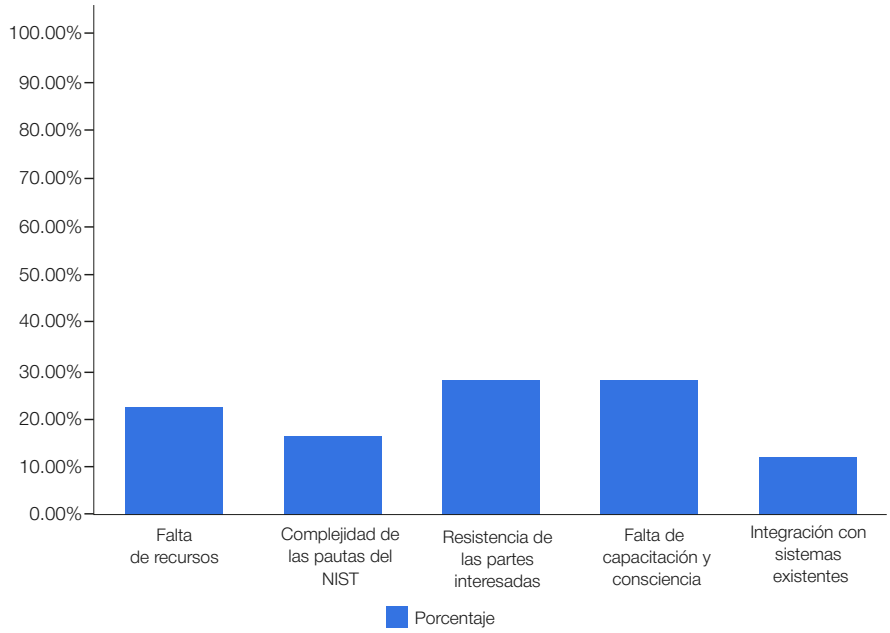


Figure 5: RMF Retos, Creación

Pregunta 11b: Si no está planeando crear un RMF, ¿por qué no?

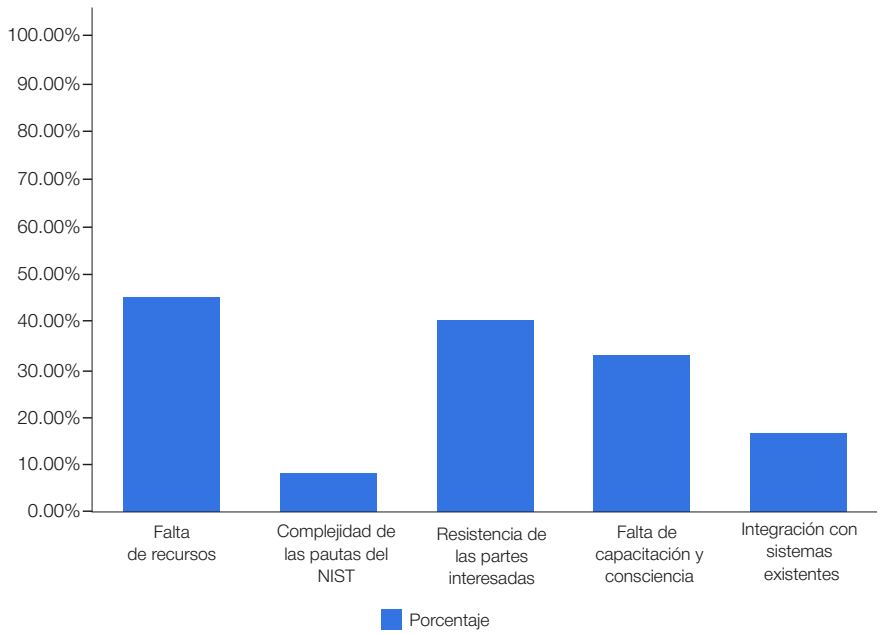


Figure 6: RMF Desafíos, barrera de entrada

En general, el 94% de los encuestados estuvo al menos algo de acuerdo en que la implementación de un RMF puede mejorar la resiliencia de su organización contra amenazas cibernéticas como el ransomware. Esto pone de manifiesto el consenso entre los profesionales sobre la importancia de una RMF y cómo puede disminuir el riesgo. De los encuestados que emplearon un RMF, la mayoría utilizó ISO 27001 (39%) y NIST (38%), y otro 17% utilizó controles CIS. Los tres marcos más populares proporcionan capacidades similares pero únicas a una organización, según el tamaño, el presupuesto, la ubicación y más. Una recomendación de este informe es emplear lo que se adapte a la organización en cuestión, pero asegurarse de que permite la interoperabilidad, dependiendo del campo de la organización, el país y otros factores.

La implementación de un RMF puede ayudar a una organización de muchas maneras. La mayoría de los encuestados (83%) cree que un RMF hace más por la seguridad proactiva que tener una respuesta/recuperación mejor o más rápida (15%). La mayoría de los encuestados (46%) respondieron que "Reducir el riesgo de ataques" es la parte más valiosa de un RMF, y otro gran grupo (36%) afirmó que "Una mejor preparación" proporciona el mayor valor. La "recuperación más rápida" (11%) y la "respuesta más rápida" (4%) se consideraron menos importantes que la proactividad. Es comprensible que los CISO y otros profesionales prefieran prevenir un ataque que gestionar sus repercusiones. Uno de los beneficios del NIST CSF y otros RMF es que preparan a una organización para ambos. La proactividad y la preparación, tanto en términos de software como de formación, son esenciales. Sin embargo, es imposible evitar que se produzcan todos los ataques. Como tal, se recomienda encarecidamente la implementación de un RMF que mitigue el riesgo y lo prepare para un ataque.

De los que respondieron a la encuesta, el 72% afirmó que había implementado un RMF en la estrategia de ciberseguridad de su organización. La mayoría de ellos (40% del total) coincidieron en que ha sido muy eficaz, y algunos (30% del total) afirmaron que ha tenido una eficacia limitada. Otro 23% de los encuestados afirmó que no había implementado un RMF, pero lo está considerando, y solo el 4% de los encuestados afirmó que no tenía planes de implementar uno. Este resultado enfatiza el consenso en la región sobre la utilización de algún RMF para mitigar el riesgo y prepararse para un posible ataque.

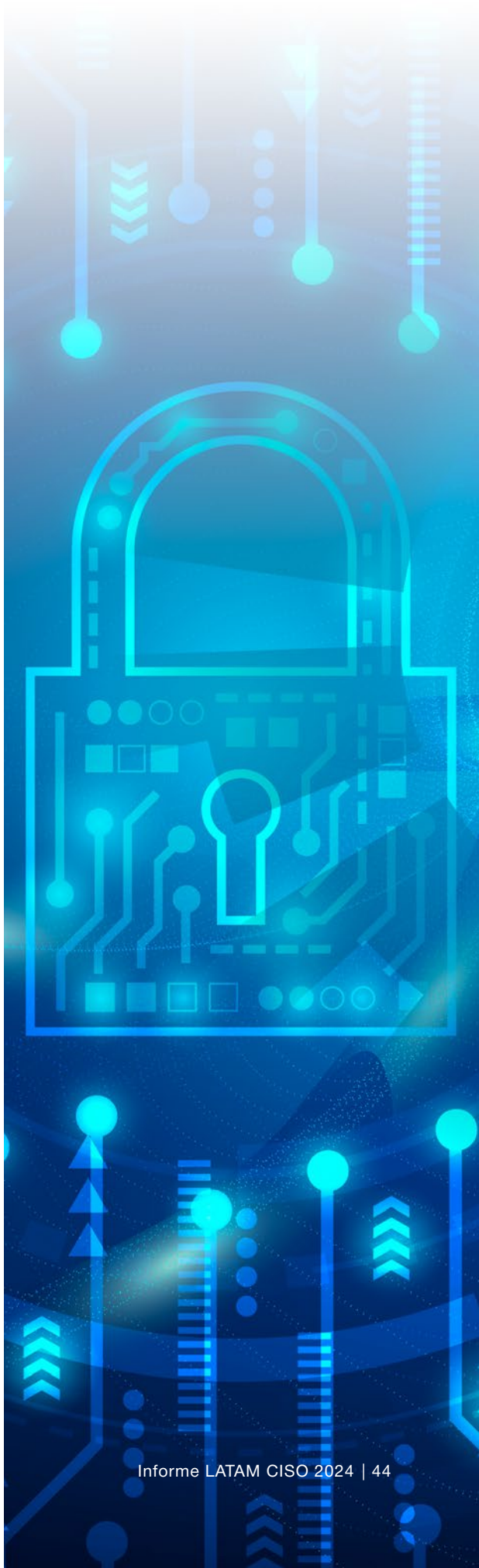
Al filtrar por sector público frente a privado, aparece una ligera diferencia. De los que trabajaban en el sector público, el 60% había implementado un RMF, con una división relativamente equitativa entre una eficacia alta y una eficacia limitada. Sin embargo, en el sector privado, el 80% de los encuestados informaron haber implementado un RMF, con la mayoría (46% frente a 34%) reportando una alta efectividad sobre una efectividad limitada. Lo más probable es que esta diferencia en los resultados se pueda atribuir a una diferencia de recursos, mentalidad o personal entre los sectores público y privado.

En cuanto a los desafíos que enfrentan quienes han implementado un RMF y los desafíos esperados por quienes no lo han implementado, la complejidad de las regulaciones o la dificultad para implementarlas se calificaron como extremadamente bajas. La respuesta menos

representada a la pregunta 11a, "¿Qué desafíos, si los hay, ha encontrado al considerar la creación de un RMF?", fue "La complejidad de las pautas del NIST" con solo el 11%. Lo que las personas han encontrado difícil es completamente solucionable. Los dos retos más comunes a los que se enfrentaron fueron "Resistencia de las partes interesadas" y "Formación y concienciación insuficientes", cada uno con un 25%, mientras que "Integración con los sistemas existentes" fue del 16%. La distribución más o menos equitativa de estas cuestiones pone de relieve el hecho de que no existe un problema singular al que se enfrenten las organizaciones que intentan implementar un RMF. Además, la mayoría de los problemas son institucionales (resistencia de las partes interesadas o falta de capacitación, conciencia y recursos), en contraposición a los problemas con el marco en sí. El aumento de la concienciación, los programas de capacitación y la elaboración de presupuestos son formas de mejorar el resultado de un RMF.

De los encuestados que informaron que no planeaban crear un RMF, sus creencias sobre posibles problemas coincidían relativamente bien con lo que otros informaron como problemas reales. La principal diferencia es que, de los que no tienen la intención de crear un RMF, el mayor problema fue la "Falta de Recursos" (33%). En muchos casos, la falta de recursos puede ser una barrera de entrada importante para la implementación de un RMF.

Cabe destacar que la complejidad del marco del NIST, por ejemplo, no es la razón por la que la gente haya optado por no crear un RMF.



Nube pública

Pregunta 12: ¿Su organización utiliza actualmente una nube pública?

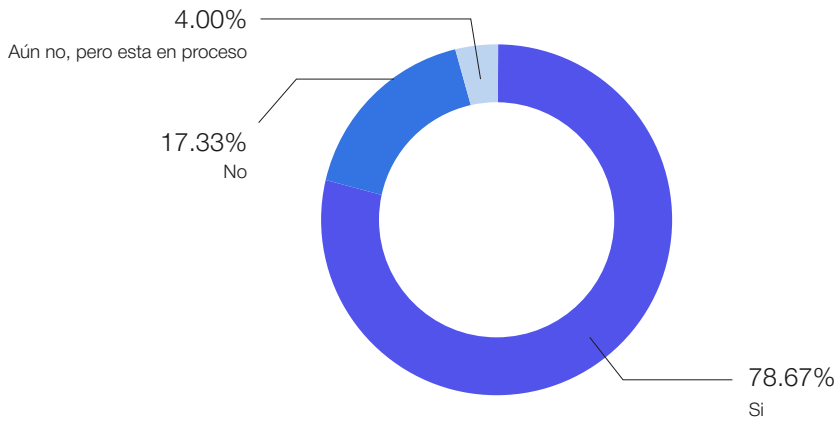


Figura 7: Adopción de la nube pública

Pregunta 13: ¿Fue la seguridad una de las principales motivaciones para migrar a la nube?

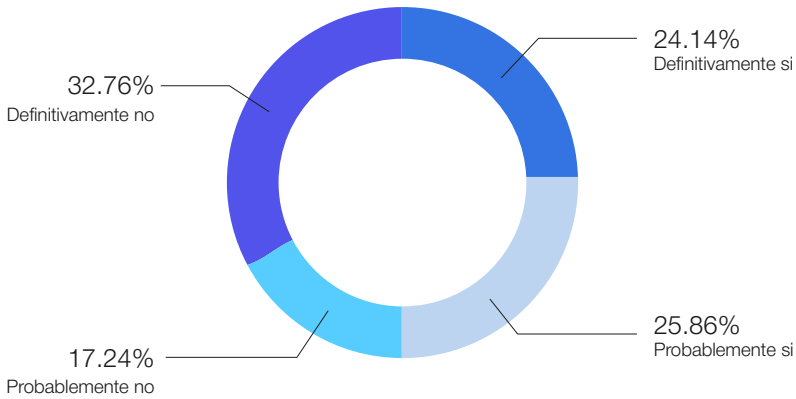


Figura 8: La seguridad como motivador

Pregunta 14: ¿Cree que sus sistemas son más seguros en la nube?

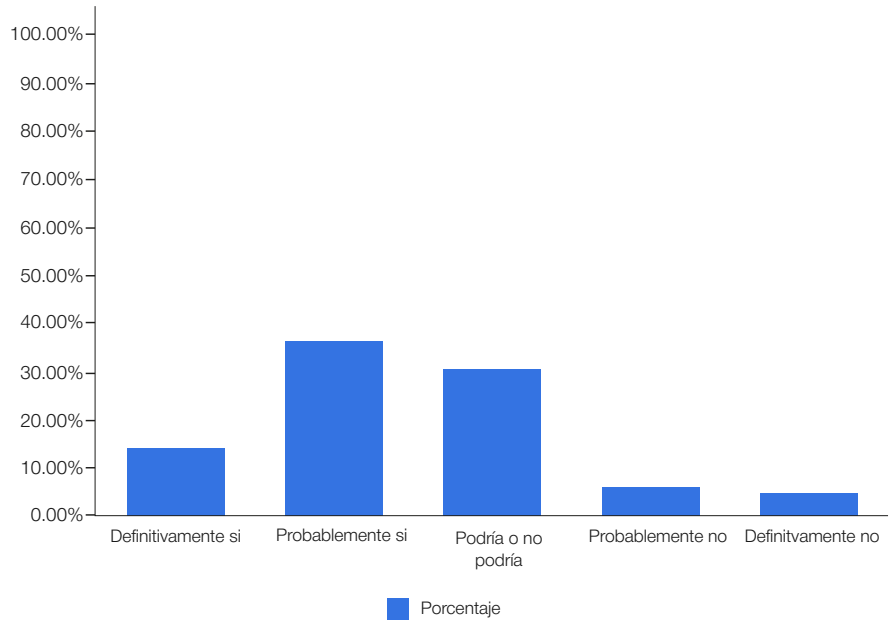


Figura 9: Seguridad en la nube

Pregunta 15: ¿Cree que la computación en la nube es más eficaz para mitigar los ataques de ransomware?

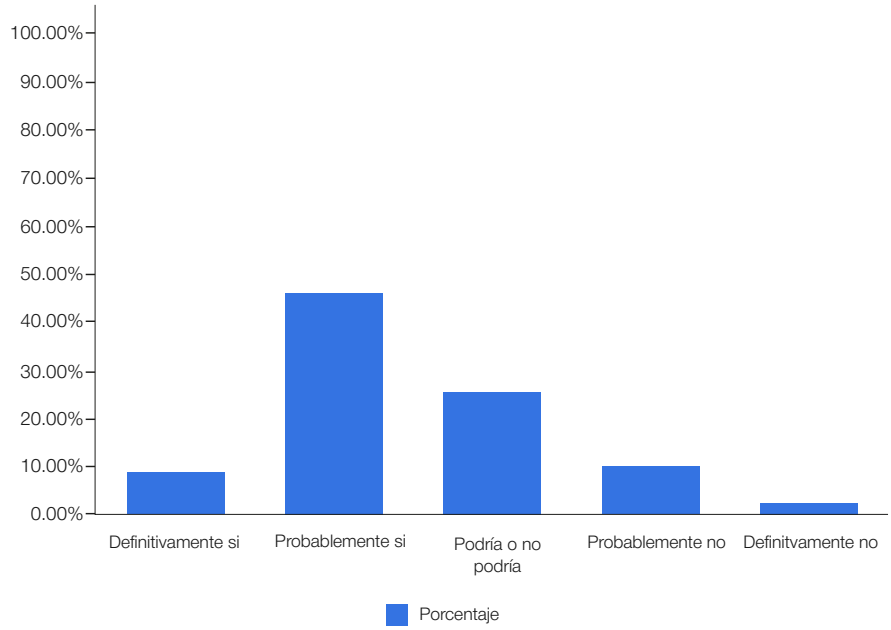


Figura 10: Computación en la nube para mitigar el ransomware

Pregunta 18: Si tuviera que migrar a la nube, ¿sentiría que es más segura?

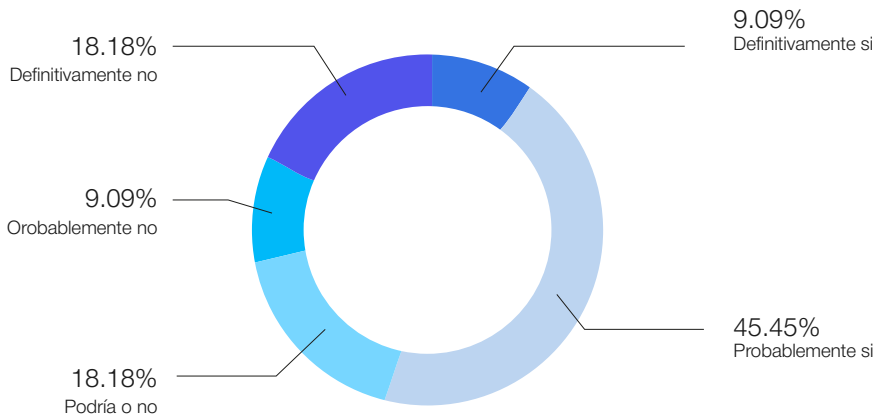


Figura 11: Seguridad en la nube, potencial

Pregunta 19: ¿Es el ransomware una preocupación a la hora de decidir si migrar a la nube?

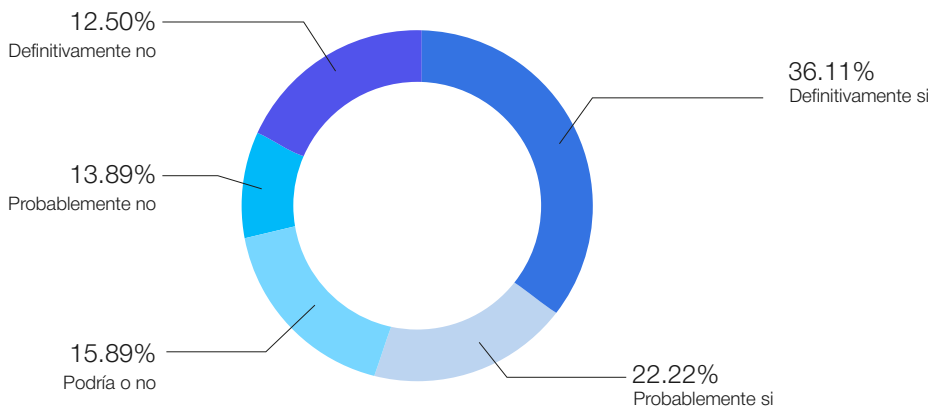


Figura 12: El ransomware como barrera para la nube

Más del 82% de los encuestados afirmaron que su organización utilizaba actualmente servicios de infraestructura de ciberseguridad basados en la nube (nube pública; 78%) o estaban en proceso de implementarlos (4%). Una vez más, existe una diferencia entre el sector público y el privado con respecto a los servicios de nube pública. El sector público, tal vez con menos recursos o más requisitos gubernamentales que cumplir, informó de una menor ejecución. En concreto, solo el 62% informó que actualmente utiliza servicios de nube pública, mientras que otro 5% estaba en proceso de implementarlos. Sin embargo, en el sector privado, más del 88% de los encuestados había implementado una nube pública, y otro 2% estaba en proceso.

Las respuestas indican la creencia de que el uso de servicios en la nube disponibles comercialmente podría proporcionar más seguridad contra los ataques. Por ejemplo, el 50% de los encuestados afirmó que la seguridad era uno de los principales motivadores para migrar a la nube. Hay muchos factores a tener en cuenta a la hora de migrar a la nube, pero la mejora de la seguridad parece haber sido una prioridad para los encuestados. Confirmando esto, la mayoría de los encuestados sintieron que sus sistemas eran más seguros en la nube, con un 36% respondiendo "probablemente sí" y otro 12% diciendo "definitivamente sí" a la pregunta: "Si tuviera que migrar a la nube, ¿sentiría que es más segura?" Sin embargo, un gran porcentaje (36%) no estaba seguro.

Del mismo modo, más de la mitad (57%) de los encuestados cree que la computación en la nube es "probablemente" (48%) o "definitivamente" (9%) más eficaz para mitigar los ataques de ransomware, mientras que el 29% afirmó que podría o no serlo. Como tal, la mayoría de los encuestados tenían cierta confianza en las capacidades de migrar a la nube para mitigar el ransomware y otros ataques cibernéticos de manera más efectiva.

Para finalizar las reflexiones de los encuestados, parece que hay un consenso sobre la migración a la nube. Todavía existe cierta incertidumbre con respecto a la cantidad exacta de mayor seguridad que proporciona, pero quienes participaron en esta encuesta, que incluyen CISO y otros con conocimiento de los sistemas de sus organizaciones, son optimistas.

Los encuestados coincidieron en la importancia de implementar un RMF y en el potencial de la migración a servicios de nube pública disponibles comercialmente. Para enfatizar un tema común entre las preguntas relacionadas con los RMF y la nube, la complejidad y la dificultad de implementación no son los mayores desafíos que enfrentan. Más bien, los problemas institucionales, como la escasez de personal, los problemas de capacitación o la resistencia de las partes interesadas, son los que impiden que las organizaciones se protejan y se preparen para los ciberataques, como el ransomware.

Recomendaciones de política

Recomendación #1: Inversión en el desarrollo de capacidades humanas

A partir de las entrevistas y las respuestas a la encuesta, se evidenció que los CISO de América Latina comparten una profunda preocupación por la insuficiente capacitación y la conciencia sobre las amenazas cibernéticas. Este estudio recomienda que los gobiernos asignen fondos en su año fiscal para equipar a los empleados públicos con herramientas y conocimientos de ciberseguridad en la mitigación de riesgos de ciberseguridad. Este enfoque integrado abordaría la actual brecha de habilidades y la falta de capacidad en las prácticas de ciberseguridad, garantizando la actualización continua de habilidades y conocimientos en la mitigación de riesgos de ciberseguridad. Esta recomendación también aprovecharía métodos rentables de mitigación de riesgos mediante una mayor concienciación del personal.

Recomendación # 2: Establecimiento de un RMF Voluntario

Varios países de LATAM han tomado medidas para desarrollar marcos de ciberseguridad como parte de sus agendas digitales. Sin embargo, muchas agencias gubernamentales no están obligadas a reportar incidentes o seguir las mejores prácticas. La recomendación de un RMF voluntario combinaría el establecimiento de una agencia de ciberseguridad de gobernanza mixta, un CSIRT nacional, en los países que aún no lo han implementado, y la creación de bases de datos de incidentes sectoriales específicos. La creación de la agencia y el equipo de respuesta se combinaría con acciones legislativas y regulatorias, como la promulgación de leyes integrales de ciberseguridad, la implementación de requisitos obligatorios de notificación de incidentes de ciberseguridad en una ubicación centralizada y la provisión de incentivos para la participación del sector privado en iniciativas de ciberseguridad. Este enfoque dual proporcionaría una protección específica para las infraestructuras críticas y exigiría las prácticas de ciberseguridad necesarias, como la notificación de incidentes y la asignación presupuestaria para la formación en ciberseguridad.

Los países latinoamericanos pueden utilizar estructuras establecidas de diferentes países como punto de partida o basar directamente sus marcos en estas estructuras. Si bien los países latinoamericanos tienen diferencias en

la fuerza laboral, las estrategias cibernéticas existentes, los aliados/enemigos geopolíticos y más, la construcción de RMF similares beneficiaría a la región de muchas maneras. Un enfoque es desarrollar un RMF basado directamente en el NIST, como la Metodología de Defensa Cibernética de Israel o el Marco Nacional de Seguridad Cibernética de Italia. Otro enfoque es seguir el ejemplo de algunos países latinoamericanos, como Uruguay y Colombia, analizando el NIST y utilizando sus ideas centrales en estrategias de ciberseguridad personalizadas. Los cinco pilares principales del CSF son "Identificar, Proteger, Detectar, Responder y Recuperar". Independientemente del tamaño de una organización o de la RMF que se elija, seguir estos principios fundamentales y establecer una RMF aumentará la solidez de la ciberseguridad.

Recomendación # 3: Inversión Estratégica en Infraestructura y Tecnologías de Ciberseguridad

En tercer lugar, la inversión estratégica en infraestructura y tecnologías de ciberseguridad abarca la inversión en tecnología de ciberseguridad y la adopción de soluciones de nube pública, al tiempo que se tiene en cuenta lo que está en juego en cuanto a quién tiene el control. Esta recomendación reconoce la necesidad de adaptarse a la evolución de las ciberamenazas y a la creciente digitalización de los sectores. Por lo tanto, este estudio aboga por la inversión en tecnologías que equilibren las necesidades de seguridad con la eficiencia operativa, incluida la adopción de servicios de nube pública para disminuir el riesgo de ciberseguridad y promover una transferencia segura de datos. Además, los gobiernos podrían adoptar políticas que den prioridad a la nube como medio para aprovechar los beneficios de seguridad mejorados que brindan las ofertas de nube pública. Una parte significativa de los encuestados informó haber visto disminuciones en los riesgos asociados con la adopción de la nube pública. Por lo tanto, las organizaciones y entidades gubernamentales deben evaluar cuidadosamente estos beneficios y considerar aprovechar las soluciones en la nube como parte de su estrategia de ciberseguridad.

Recomendación #4: Sistemas centralizados de gestión e informes de ciberseguridad

Los sistemas centralizados de informes y capacitación mejoran la colaboración entre diferentes sectores y agencias, agilizando la comunicación y respondiendo a incidentes de ciberseguridad. A través de esta información y capacitación centralizada, los diferentes sectores y agencias pueden observar las tendencias de manera más efectiva y responder con mayor precisión. Esta recomendación también incluye la centralización de los mecanismos de respuesta, la mejora de la eficacia en la gestión de los ciberataques y la facilitación del intercambio dinámico de información y la cooperación tanto a nivel nacional como regional. Un enfoque es que los gobiernos exijan la notificación de los ciberataques dentro de un plazo razonable. Este enfoque ayudaría a desestigmatizar el hecho de ser víctima de ataques y alentaría a las empresas a revelar los ataques en lugar de mantenerlos confidenciales. Además, este enfoque mejoraría el conocimiento de la situación y la postura de ciberseguridad a través del conocimiento colectivo y los recursos compartidos.

[i] Fundación Academia de Gobierno Electrónico. "NCSI :: Clasificación". *Ncsi.ega.ee*, ncsi.ega.ee/ncsi-index/.
[ii] Editor, CSRC Content. "Infraestructura Crítica - Glosario: CSRC". *Editor de contenido de CSRC*, csrc.nist.gov/glossary/term/critical_infrastructure.

[iii] Banco Interamericano de Desarrollo y Organización de los Estados Americanos. "*Informe: Riesgos de ciberseguridad, avances y el camino a seguir en América Latina y el Caribe".* 27 de julio de 2020, https://doi.org/10.18235/0002513.
[iv] Banco Interamericano de Desarrollo y Organización de los Estados Americanos, 2020.
[v] Vicens, A. J. "Los gobiernos de América Latina son los principales objetivos del ransomware debido a la falta de recursos, argumenta un análisis". *CyberScoop*, 16 de junio de 2022, cyberscoop.com/latin-america-ransomware-recorded-future/.
[vi] Greig, Jonathan. "Varios ministerios del gobierno colombiano se ven obstaculizados por un ataque de ransomware". Therecord.media, 15 de septiembre de 2023, therecord.media/colombia-government-ministries-cyberattack..
[vii] Sweigart, Emilie y Jack Quinn. "¿Por qué América Latina es tan vulnerable a los ciberataques? Hicimos los números". *Americas Quarterly*, 25 de julio de 2023, americasquarterly.org/article/why-is-latin-america-so-vulnerable-to-cyberattacks-we-ran-the-numbers/.
[viii] "Estrategia de seguridad: de la infraestructura crítica nacional 2022-2032", Brigadier General Edgar Alexander Salamanca Rodríguez, General (R) Fabricio Cabrera Ortiz, Stefan Reit - Bogotá: Editorial ESDEG, Fundación Konrad Adenauer KAS, 2022.

[ix] "Lineamientos Generales Para Fortalecer la Governanza de la Seguridad Digital, la Identificación de Infraestructuras Críticas Cibernéticas y Servicios Esenciales, la Gestión de Riesgos y la Respuesta a Incidentes de Seguridad Digital". Decreto Number 338.
[x] "Ley 1273 de 2009 -Legislacion Colombiana Lexbase". *www.lexbase.co*, www.lexbase.co/lexdocs/indice/2009/l1273de2009#:~:text=%22%20LEY%201273%20DE%202009%20(enero.
[xi] "Ley 1273 de 2009 -Legislación Colombiana Lexbase".
[xii] "Ley 1273 de 2009 -Legislación Colombiana Lexbase".
[xiii] Díaz Acevedo, Martín. (2023). La evolución de la estrategia de ciberseguridad de Colombia 2011-2021. 10.13140/RG.2.2.22241.58723.
[xiv] Consejo Nacional De Política Económica Y Social República De Colombia Departamento Nacional De Planeación. "*Documento CONPES 3701 Número* 1". 14 Jul. 2011.
[xv] Díaz Acevedo, Martín. (2023).
[xvi] "Autorizacion A La Nacion Para Contratar Operaciones De Credito Externo Hasta Por La Suma De Us$ 500 Millones O Su Equivalente En Otras Monedas". Republica De Colombia, Departamento Nacional de Planeacion.
[xvii] Secretaria Juridica Distrital. "Decreto 620 de 2019 Alcaldía Mayor de Bogotá, D.C.". *www.alcaldiabogota.gov.co*, 18 Oct. 2019, www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=87246.
[xviii] Ministerio De Tecnologias de la Información y Las Comunicaciones. "DECRETO N° 620 de 2020". *Dapre.presidencia.gov.co*, 2 Mayo 2020, dapre.presidencia.gov.co/normativa/normativa/DECRETO%20620%20DEL%202%20DE%20MAYO%20DE%202020.pdf.
[xix] Ministerio de Ambiente y Desarrollo Sostenido. "Política de Protección de Datos Personales". *Ministerio de Ambiente Y Desarrollo Sostenible*, 13 Oct. 2022, www.minambiente.gov.co/politica-de-proteccion-de-datos-personales/#:~:text=Ley%20de%20Protecci%C3%B3n%20de%20Datos.
[xx] CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL REPÚBLICA DE COLOMBIA. "CONPES 3995- POLÍTICA NACIONAL de CONFIANZA Y SEGURIDAD DIGITAL". *Colaboracion.dnp.gov.co*, 1 Julio 2020, colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf.
[xxi] "ABC SEGURIDAD DIGITAL Decreto 338 de 2022". MinTic. 2022.

[xxii] "Decreto 767 del 16 de mayo de 2022: la Nueva Política de Gobierno Digital". MinTiC.
[xxiii] Sandoval, Cath. "Todo lo que debe saber sobre los habilitadores tecnológicos en los seguros". *LISA Insurtech*, 9 de febrero de 2021, lisainsurtech.com/know-everything-about-the-impact-of-technology-enablers/#:~:text=A%20technology%20enabler%20is%20a. Consultado el 2 de abril de 2024.
[xxiv] "Ciberseguridad a La Medida, La Apuesta de Claro". *www.claro.com.co*, 2 Nov. 2023, www2.claro.com.co/empresas/sectores/noticias-interes/ciberseguridad-a-la-medida/.
[xxv] Puentes León, Sthefanie. *Colombia: ¿Es Un Estado Efectivo En Términos De Seguridad Digital Con Énfasis En El Sector Privado?* Junio 2019.
[xxvi] Puentes León, Sthefanie. (2019).
[xxvii] Ochoa, Gladys & Becerra, Jairo & Sanchez Acevedo, Marco Emilio & M., Carlos & Keeney, Alejandro & Páez, Rafael V. & Contreras Fernández, Aristides & León, Ivonne. (2019). La Seguridad en el Ciberespacio, Un desafío para Colombia. Capítulo V. Gestión de Riesgo en Seguridad Digital en el Sector Privado y Mixto - Contexto General.. 10.25062/9789585216549.
[xxviii] Ochoa, Gladys & Becerra, Jairo & Sanchez Acevedo, Marco Emilio & M., Carlos & Keeney, Alejandro &Páez, Rafael V. & Contreras Fernández, Aristides &León, Ivonne. (2019).
[xxix] Ochoa, Gladys & Becerra, Jairo & Sanchez Acevedo, Marco Emilio & M., Carlos & Keeney, Alejandro & Páez, Rafael V. & Contreras Fernández, Aristides & León, Ivonne. (2019). La Seguridad en el Ciberespacio, Un desafío para Colombia. Capítulo V. Gestión de Riesgo en Seguridad Digital en el Sector Privado y Mixto - Contexto General. 10.25062/9789585216549.
[xxx] "LEY 1928 de 2018". *Suin-Juriscol.gov.co* de 2018, www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/30035501.

[xxxi] Consejo de Europa. "Convención de Budapest y normas conexas". *Cibercrimen*, 2014, www.coe.int/en/web/cybercrime/the-budapest-convention.
[xxxii] Consejo de Europa. *Convenio sobre el Delito Cibernético*. 23 de noviembre de 2001.
[xxxiii] Consejo de Europa. *Convenio sobre el Delito Cibernético*. 23 de noviembre de 2001.
[xxxiv] "ABC Del Acuerdo Comercial Con Israel | TLC". *Tlc.gov.co*, 2021, www.tlc.gov.co/preguntas-frecuentes/abc-del-acuerdo-comercial-con-israel.
[xxxv] Banco Interamericano de Desarrollo. "BID | Israel se compromete con la iniciativa de ciberseguridad del BID en América Latina y el Caribe" www.iadb.org, 24 de febrero de 2022, www.iadb.org/en/news/israel-commits-idb-cybersecurity-initiative-latin-america-and-caribbean#:~:text=Through%20a%20%242%20million%20contribution.
[xxxvi] Ministerio de Relaciones Exteriores. "Colombia Fue Elegido Como Primer Presidente Del Grupo de Trabajo Sobre Medidas de Fomento de Cooperación Y Confianza En El Ciberespacio de La OEA | Cancillería". *www.cancilleria.gov.co*, 2 Mar. 2018, www.cancilleria.gov.co/newsroom/news/colombia-fue-elegido-primer-presidente-grupo-trabajo-medidas-fomento-cooperacion.
[xxxvii] "Unión Internacional de Telecomunicaciones | Misión Permanente de Colombia". *Ginebra-Onu.mision.gov.co*, ginebra-onu.mision.gov.co/en/international-telecommunications-union#:~:text=ITU%20was%20founded%20in%20Paris%20in%201865.
[xxxviii] Administración de Comercio Internacional. "Perspectivas de ciberseguridad en Colombia", www.trade.gov, 25 de febrero de 2021, www.trade.gov/market-intelligence/colombia-cybersecurity-outlook.

[xl] Kiuwan. "Filtraciones de datos y países de LATAM | Kiuwan". www.kiuwan.com, 14 de marzo de 2023, www.kiuwan.com/blog/latam-data-breaches-top-3-countries-affected/.
[xli] Kiuwan. "Filtraciones de datos en LATAM: los 3 principales países afectados".
[xlii] Kiuwan. "Filtraciones de datos en LATAM: los 3 principales países afectados".
[xliii] Greig, Jonathan. "Varios ministerios del gobierno colombiano se ven obstaculizados por un ataque de ransomware".
[xliv] Greig, Jonathan. "Varios ministerios del gobierno colombiano se ven obstaculizados por un ataque de ransomware".
[xlv] Reuters. "Más de 50 entidades estatales y privadas colombianas afectadas por ciberataque -Petro". Reuters, 18 de septiembre de 2023, www.reuters.com/world/americas/more-than-50-colombian-state-private-entities-hit-by-cyberattack-petro-2023-09-18/.
[xlvi] Reuters. "Más de 50 entidades estatales y privadas colombianas afectadas por ciberataque -Petro".
[xlvii] Thomas, Roland. "Colombia se defiende de un devastador ataque de ransomware | Thomas Murray". Thomasmurray.com, thomasmurray.com/insights/colombia-fights-back-devastating-ransomware-attack.
[xlviii] Thomas, Roland. "Colombia se defiende de un devastador ataque de ransomware"
[xlix] Thomas, Roland. "Colombia se defiende de un devastador ataque de ransomware"

[l] Díaz, Laura Lesmes. "Los Pilares y Claves Del Proyecto Para La Creación de La Agencia de Seguridad Digital". *El Tiempo*, El Tiempo, 26 Julio 2023, www.eltiempo.com/tecnosfera/novedades-tecnologia/los-pilares-y-claves-del-proyecto-para-la-creacion-de-la-agencia-de-seguridad-digital-790038.

[li] Comercio Comisión Europea. *Sector de Ciberseguridad en Centroamérica*. Noviembre de 2022.
[lii] Sistema Costarricense de Información Jurídica. "Reforma de La Sección VIII, Delitos Informáticos Y Conexos, Del Título VII Del Código Penal N° 9048". *www.pgrweb.go.cr*, 7 Oct. 2012, www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=73583.
[liii] "Estrategia Nacional de Ciberseguridad – Costa Rica". Ministerio de Ciencia, Tecnología y Telecomunicaciones. Año 2017.
[liv] "LEY DE PROTECCIÓN DE LA PERSONA FRENTE AL TRATAMIENTO DE SUS DATOS PERSONALES", chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.oas.org/es/sla/ddi/docs/CR4%20Ley%20de%20Protecci%C3%B3n%20de%20la%20Persona%20frente%20al%20Tratamiento%20de%20sus%20Datos%20Personales.pdf

[lv] S-COM: Davinsson Nunjar Flores. “Sistema Costarricense De Información Jurídica”. *S-COM*, www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989&strTipM=TC.

[lvi] OCDE. *Gobernanza Pública en Costa Rica*. PUBE. Año 2021.

[lvii] OCDE. (2021).

[lviii] Ministerio de Ciencia, Tecnología y Telecomunicaciones. (2017)

[lix] Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones. *Estrategia Nacional de Ciberseguridad de Costa Rica* 2023 - 2027. 10 de noviembre de 2023.

[lx] Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones. (2023).

[lxi] Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones. (2023).

[lxii] Cybersec: "el clúster que reunió a las principales empresas y organizaciones de ciberseguridad de la región". CINDE Agencia de Promoción de Inversiones de Costa Rica, www.cinde.org/en/essential-news/cybersec-the-cluster-that-brought-together-the-regions-top-cybersecurity-companies-and-organizations.

[lxiii] Cybersec: "el clúster que reunió a las principales empresas y organizaciones de ciberseguridad de la región". (2022)

[lxiv] Society, European Foundation for Information. *“Ministerio de Economia, Industria y Comercio de Costa Rica”. Ministerio de Economía, Industria y Comercio de Costa Rica -*, 28 Feb. 2022, www.meic.go.cr/comunicado/1120/programa-nacional-de-clusteres-recibe-declaratoria-de-interes-publico.php.

[lxv] "CINDE | Invertir en Costa Rica". Cinde.org, 2020, www.cinde.org/en/our-services.

[lxvi] "CINDE | Invertir en Costa Rica". (2020)

[lxvii] Fundación Europea para la Información. (2022)

[lxviii] "OEA y Trend Micro firman acuerdo para mejorar la seguridad cibernética en las Américas". Organización de los Estados Americanos, 13 de octubre de 2015, www.oas.org/en/media_center/press_release.asp?sCodigo=E-063/15.

[lxix] Portal Interamericano de Cooperación sobre Delito Cibernético (Iniciativa deteriorada)". *Organización de los Estados Americanos*, https://scm.oas.org/pdfs/2019/CICTE1301B.pdf.

[lxx] GTCA de las Naciones Unidas 2021-2025 2ª Sesión Sustantiva". Geneva Digital Watch, dig.watch/event/un-oewg-2021-2025-2nd-sustantive-session/un-oewg-2021-2025-international-law.

[lxxi] Reloj digital de Ginebra. "[Evento] GTCA de la ONU 2021-2025 2ª Sesión Sustantiva".

[lxxii] "Costa Rica". Agencia de Cooperación Internacional del Japón, www.jica.go.jp/english/overseas/costarica/index.html.

[lxxiii] https://www.rree.go.cr/?sec=servicios&cat=prensa&cont=593&id=6008

[lxxiv] "Costa Rica será sede de la tercera conferencia regional de la Convención de Budapest sobre Delito Cibernético". *Ministerio de Relaciones Exteriores y Culto, Gobierno de Costa Rica*, www.rree.go.cr/?sec=servicios&cat=prensa&cont=593&id=6008.

[lxxv] Tornaghi, Cecilia. "El Dramático Ciberataque Que Puso a América Latina En Alerta". *Americas Quarterly*, 25 Julio 2023, americasquarterly.org/article/el-dramatico-ciberataque-que-puso-a-america-latina-en-alerta/..

[lxxvi] “Costa Rica agradece a España y Estados Unidos el apoyo en ciberseguridad”. Forbes Centroamérica. Diciembre 2023.

[lxxvii] "Estados Unidos anuncia $25 millones para fortalecer la ciberseguridad de Costa Rica". Embajada de los Estados Unidos en Costa Rica, cr.usembassy.gov/united-states-announces-25-million-to-strengthen-costa-ricas-cybersecurity/#:~:text=Today%2C%20the%20United%20States%20and,reforzster%20Costa%20Rica's%20digital%20infrastructure.

[lxxviii] "CCrif y la Agencia Regional para la Gestión del Riesgo de Desastres de Centroamérica, Cepredenac, firman memorándum". *Oficina de las Naciones Unidas para la Reducción del Riesgo de Desastres*, UNO.ORG, www.preventionweb.net/news/ccrif-and-central-americas-regional-disaster-risk-management-agency-cepredenac-sign-memorandum.

[lxxix] Sherman, Christopher. "Costa Rica se declara en emergencia por ciberataque en curso". *AP NEWS,* Associated Press, 10 de mayo de 2022, apnews.com/article/russia-ukraine-technology-business-gangs-costa-rica-9b2fe3c5a1fba7aa7010eade96a086ea..

[lxxx] Sherman, Christopher. "Costa Rica se declara en emergencia por ciberataque en curso". (2022).

[lxxxi] Sherman, Christopher. "Costa Rica se declara en emergencia por ciberataque en curso". (2022).
[lxxxii] "Ataque de ransomware en Costa Rica (2022)". CCDCOE, https://cyberlaw.ccdcoe.org/wiki/Costa_Rica_ransomware_attack_(2022)#cite_note-8.
[lxxxiii] Ataque de ransomware en Costa Rica (2022).
[lxxxiv] Ataque de ransomware en Costa Rica (2022).
[lxxxv] Datta, P. M., & Acton, T. (2022). Ransomware y la emergencia nacional en Costa Rica: un marco de defensa y un caso de enseñanza. *Revista de Casos de Enseñanza de Tecnologías de la Información*, 0(0). https://doi.org/10.1177/20438869221149042
[lxxxvi] Burgess, Matt. "El ataque de Conti contra Costa Rica desencadena una nueva era de ransomware". WIRED UK, 12 de junio de 2022, www.wired.co.uk/article/costa-rica-ransomware-conti.

[lxxxvii] Pratim Milton Datta y Thomas Acton, "Ransomware y la emergencia nacional de Costa Rica: *un marco de defensa y un caso de enseñanza"* (2023) Revista de Casos de Enseñanza de Tecnología de la Información 1.
[lxxxviii] "EE.UU. compromete 25 millones de dólares a Costa Rica para la recuperación del ransomware Conti". El Registro. Marzo 2023.
[lxxxix] Pratim Milton Datta y Thomas Acton. (2023).
[xc] (Comercio Comisión Europea)
[xci] Biblioteca del Congreso Nacional de Chile. "DECRETO 533 CREA COMITÉ INTERMINISTERIAL SOBRE CIBERSEGURIDAD". www.bcn.cl/Leychile, 17 Julio 2015, www.bcn.cl/leychile/navegar?idNorma=1079608&idVersion=2023-08-14..
[xcii] Biblioteca del Congreso Nacional de Chile. "DECRETO 533 CREA COMITÉ INTERMINISTERIAL SOBRE CIBERSEGURIDAD".
[xciii] Barrios Achavar, Verónica. "Política Nacional de Ciberseguridad: 2017-2022". *Biblioteca Del Congreso Nacional de Chile*, Julio 2018, pp. 1–7, obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/26760/1/POLITICA_NACIONAL_DE_CIBER.pdf.
[xciv] Barrios Achavar, Verónica. "Política Nacional de Ciberseguridad: 2017-2022".
[xcv] Biblioteca del Congreso Nacional de Chile. "Historia de La Ley No 21.113". www.bcn.cl, www.bcn.cl/historiadelaley/nc/historia-de-la-ley/vista-expandida/7585/#h2_4_1.
[xcvi] Ministerio del Interior y Seguridad Pública. Resolución Exenta No. 5.006. 20 Aug. 2019, www.csirt.gob.cl/media/2019/09/RES.-EXENTA-N-5006-CREACION-DE-DIVISION-Y-UNIDAD.pdf.
[xcvii] Ministerio del Interior y Seguridad Pública. Resolución Exenta No. 1661. 30 May 2023, https://www.csirt.gob.cl/media/2023/12/Rex-2023-RESOLUCI%C3%93N-EXENTA-1661-deja-sin-efecto-Rex-11.536-DE-2020-y-modifica-Rex-N5.006-DE-2019-ambas-de-la-SSI.pdf.
[xcviii] Ministerio del Interior y Seguridad Pública. Resolución Exenta No. 5.006.
[xcix] Ministerio del Interior y Seguridad Pública. Resolución Exenta No. 5.006.
[c] Ministerio del Interior y Seguridad Pública. Resolución Exenta No. 5.006.
[ci] Equipo de Respuesta a Incidentes de Seguridad Cibernética (CSIRT). "Quiénes Somos". Www.csirt.gob.cl, 2 de octubre de 2019, www.csirt.gob.cl/quienes-somos/.
[cii] Administración de Comercio Internacional. "Chile - Tecnologías de la Información".
[ciii] "Diario Oficial publica nueva Política Nacional de Ciberseguridad 2023-2028". CSIRT, 6 Dec. 2023, https://csirt.gob.cl/noticias/diario-oficial-publica-nueva-politica-nacional-de-ciberseguridad-2023-2028/.
[civ] Equipo Actualidad Jurídica. "Nueva Política Nacional de Ciberseguridad 2023-2028 Para Proteger La Seguridad Digital Del País". DOE | Actualidad Jurídica, 4 Dec. 2023, actualidadjuridica.doe.cl/nueva-politica-nacional-de-ciberseguridad-2023-2028-para-proteger-la-seguridad-digital-del-pais/.
[cv] El Congreso Nacional. PROYECTO DE LEY QUE ESTABLECE UNA LEY MARCO SOBRE CIBERSEGURIDAD E INFRAESTRUCTURA CRÍTICA DE LA INFORMACIÓN. 12 Dec. 2023, www.csirt.gob.cl/media/2023/12/Boletin14847-TextoFinal.pdf.
[cvi] "Avanza La Ciberseguridad En Chile: Nueva Ley Marco de Ciberseguridad E Infraestructura Crítica de La Información Es Despachada a Ley". Centro de Innovación, 21 Dec. 2023, centrodeinnovacion.uc.cl/noticias/avanza-la-

ciberseguridad-en-chile-nueva-ley-marco-de-ciberseguridad-e-infraestructura-critica-de-la-informacion-es-despachada-a-ley/.

[cvii] Fuenzalida, Cesar. (2023).

[cviii] "Congreso Aprueba Ley Marco de Ciberseguridad, Que Fortalece Institucionalidad Y Crea Agencia Nacional". CSIRT, 13 Dec. 2023, www.csirt.gob.cl/noticias/congreso-aprueba-ley-marco/.

[cix] El Congreso Nacional. PROYECTO DE LEY QUE ESTABLECE UNA LEY MARCO SOBRE CIBERSEGURIDAD E INFRAESTRUCTURA CRÍTICA DE LA INFORMACIÓN.

[cx] El Congreso Nacional. PROYECTO DE LEY QUE ESTABLECE UNA LEY MARCO SOBRE CIBERSEGURIDAD E INFRAESTRUCTURA CRÍTICA DE LA INFORMACIÓN.

[cxi] "Congreso Aprueba Ley Marco de Ciberseguridad, Que Fortalece Institucionalidad Y Crea Agencia Nacional". CSIRT.

[cxii] "Congreso Aprueba Ley Marco de Ciberseguridad, Que Fortalece Institucionalidad Y Crea Agencia Nacional". CSIRT.

[cxiii] "Congreso Aprueba Ley Marco de Ciberseguridad, Que Fortalece Institucionalidad Y Crea Agencia Nacional". CSIRT.

[cxiv] "Congreso Aprueba Ley Marco de Ciberseguridad, Que Fortalece Institucionalidad Y Crea Agencia Nacional". CSIRT.

[cxv] "Congreso Aprueba Ley Marco de Ciberseguridad, Que Fortalece Institucionalidad Y Crea Agencia Nacional". CSIRT.

[cxvi] "Congreso Aprueba Ley Marco de Ciberseguridad, Que Fortalece Institucionalidad Y Crea Agencia Nacional". CSIRT.

[cxvii] "Alianza Chilena de Ciberseguridad". Alianzaciberseguridad.cl, alianzaciberseguridad.cl/.

[cxviii] "Nosotros – INCIB Chile". Instituto Nacional de Ciberseguridad de Chile, 2021, incibchile.cl/nosotros/.

[cxix] "Nuestra Asociación". Chiletec. https://chiletec.org/sobre-chiletec/nuestra-asociacion.

[cxx] "El Convenio de Budapest (STE Nº 185) y sus Protocolos". Consejo de Europa, 2014, www.coe.int/en/web/cybercrime/the-budapest-convention.

[cxxi] "9° Congreso Latinoamericano Tecnología Y Negocios America Digital 2024". Congreso America Digital, 2021, congreso.america-digital.com/.

[cxxii] Techbound Technology, "Alerta de ciberseguridad: el ciberataque de IFX Networks sacude a Colombia, Chile y Argentina", 15 de septiembre de 2023, https://www.linkedin.com/pulse/cybersecurity-alert-ifx-networks-cyberattack-shakes/.

[cxxiii] "Ejercito de Chile Es Atacado Por La Nueva Banda de Ransomware Rhysida". CronUp Ciberseguridad, 29 Mayo 2023, www.cronup.com/ejercito-de-chile-es-atacado-por-la-nueva-banda-de-ransomware-rhysida/.

[cxxiv] Gatlán, Sergiu . "Rhysida Ransomware filtra documentos robados del Ejército de Chile". *BleepingComputer*, 15 de junio de 2023, www.bleepingcomputer.com/news/security/rhysida-ransomware-leaks-documents-stolen-from-chilean-army/.

[cxxv] "Ejercito de Chile Es Atacado Por La Nueva Banda de Ransomware Rhysida". CronUp Ciberseguridad.

[cxxvi] "Alerta de Seguridad de La Información | Ransomware En Aduanas". CSIRT, 17 Oct. 2023, www.csirt.gob.cl/noticias/10cnd23-00112-01/.

[cxxvii] "Alerta de Seguridad de La Información | Ransomware En Aduanas". (2023); "Superada Alerta Informática en sistemas de Aduanas", Chile Aduanas, 10 Noviembre 2023, https://www.aduana.cl/superada-alerta-informatica-en-sistemas-de-aduanas/aduana/2023-11-10/140942.html.

[cxxviii] "Alerta de Seguridad de La Información | Ransomware En Aduanas". (2023)

[cxxix] Administración de Comercio Internacional. "Chile - Tecnologías Ambientales". *www.trade.gov,* 30 de septiembre de 2022, www.trade.gov/country-commercial-guides/chile-environmental-technologies.

[cxxx] Fundacion País Digital. "Chile Desaprovecharía Hasta US$13 Mil Millones En Crecimiento Si No Prepara a Las Personas En Habilidades Del Mercado Del Futuro Según Informe de Accenture Y Fundación País Digital – Fundación País Digital". *Fundación País Digital,* 15 Mayo 2020, paisdigital.org/2020/05/15/chile-desaprovecharia-hasta-us13-mil-millones-en-crecimiento-si-no-prepara-a-las-personas-en-habilidades-del-mercado-del-futuro-segun-informe-de-accenture-y-fundacion-pais-digital/.

[cxxxi] "Consulta Ciudadana: Guía Para El Uso de Servicios En La Nube Para La Administración Del Estado". Digital.gob.cl, 2024, participacion.digital.gob.cl/es-CL/projects/consulta-ciudadana-guia-para-el-uso-de-servicios-en-la-nube-para-la-administracion-del-estado/1.

[cxxxii] Newmeyer, Kevin. "Elementos de la Estrategia Nacional de Ciberseguridad para los Países en Desarrollo". *Revista del Instituto Nacional de Ciberseguridad*, vol. 1, no. 3, 2015, publications.excelsior.edu/publications/NCI_Journal/1-3/offline/download.pdf#page=11.
[cxxxiii] "Sobre Nosotros - CSIRT Panamá". *CSIRT Panamá - Equipo de Respuesta a Incidentes de Seguridad de La Información*, 28 Julio 2015, cert.pa/?page_id=33.
[cxxxiv] "Sobre Nosotros - CSIRT Panamá". *CSIRT Panamá - Equipo de Respuesta a Incidentes de Seguridad de La Información*, 28 Julio 2015, cert.pa/?page_id=33.
[cxxxv] "Estrategia Nacional de Seguridad Cibernética Y Protección de Infraestructura Crítica". *Autoridad Nacional Para La Innovación Gubernamental*, aig.gob.pa/descargas/2019/06/Estrategia_Nal_de_Seguridad_Cibernetica_y_Proteccion_Infraectructura_Critica.pdf.
[cxxxvi] "Sobre Nosotros - CSIRT Panamá". *CSIRT Panamá - Equipo de Respuesta a Incidentes de Seguridad de La Información*.
[cxxxvii] "Panamá: ICT Sector Fiche". *Acuerdo de Asociación UE-Centroamérica*.
[cxxxviii] "Panamá: ICT Sector Fiche". *Acuerdo de Asociación UE-Centroamérica*.
[cxxxix] "AGENDA DIGITAL ESTRATÉGICA DEL ESTADO PANAMEÑO". *Autoridad Nacional Para La Innovación Gubernamental*, 2022, aig.gob.pa/documentosaig/agenda-digital/.
[cxl] Lorenzo, Siaska. "Panamá: Desarrollos en Ciberseguridad". *DataGuidance*, 3 de mayo de 2022, www.dataguidance.com/opinion/panama-developments-cybersecurity.
[cxli] "Panamá: ICT Sector Fiche". *Acuerdo de Asociación UE-Centroamérica*, Junio 2023, trade.ec.europa.eu/access-to-markets/en/country-assets/Sector%20Fiche%20Panama%20ICT%20fv%202.pdf.
[cxlii] *Código Penal de La República de Panamá (Adoptado Por La Ley N° 14 de 18 de Mayo de 2007, Con Las Modificaciones Y Adiciones Introducidas Por La Ley N° 26 de 2008).* 21 Mayo 2008, www.wipo.int/wipolex/en/text/189272.
[cxliii] *Código Penal de La República de Panamá (Adoptado Por La Ley N° 14 de 18 de Mayo de 2007, Con Las Modificaciones Y Adiciones Introducidas Por La Ley N° 26 de 2008).* 21 Mayo 2008, www.wipo.int/wipolex/en/text/189272.
[cxliv] "Eurojust y Panamá firman un acuerdo de trabajo para intensificar la cooperación contra la delincuencia organizada". *EuroJust: Agencia de la Unión Europea para la Cooperación Judicial Penal*, 12 de enero de 2024, www.eurojust.europa.eu/news/eurojust-and-panama-sign-working-arrangement-step-cooperation-against-organised-crime.
[cxlv] "CCrif y la Agencia Regional para la Gestión del Riesgo de Desastres de Centroamérica, Cepredenac, firman memorándum". *Oficina de las Naciones Unidas para la Reducción del Riesgo de Desastres*, UNO.ORG, www.preventionweb.net/news/ccrif-and-central-americas-regional-disaster-risk-management-agency-cepredenac-sign-memorandum.
[cxlvi] "Panamá - Ciberseguridad". *www.trade.gov*, 5 de abril de 2023, www.trade.gov/country-commercial-guides/panama-cybersecurity#:~:text=Due%20to%20dramatic%20increases%20in.
[cxlvii] (Administración de Comercio Internacional, "Panamá - Ciberseguridad")
[cxlviii] Shank, Stefanie. "El Informe Global de Ciberdelincuencia 2023: Una mirada a las conclusiones clave", *Tripwire*, 17 de enero de 2024, www.tripwire.com/state-of-security/2023-global-cybercrime-report-look-key-takeaways.
[cxlix] Shank, Stefanie. "El Informe Global de Ciberdelincuencia 2023: Una mirada a las conclusiones clave", *Tripwire*, 17 de enero de 2024, www.tripwire.com/state-of-security/2023-global-cybercrime-report-look-key-takeaways.
[cl] Shank, Stefanie. "El Informe Global de Ciberdelincuencia 2023: Una mirada a las conclusiones clave" *Tripwire*, 17 de enero de 2024, www.tripwire.com/state-of-security/2023-global-cybercrime-report-look-key-takeaways.
[cli] Shank, Stefanie. "El Informe Global de Ciberdelincuencia 2023: Una mirada a las conclusiones clave", *Tripwire*, 17 de enero de 2024, www.tripwire.com/state-of-security/2023-global-cybercrime-report-look-key-takeaways.
[clii] Lorenzo, Siaska. "Panamá: Desarrollos en Ciberseguridad".
[cliii] "Informe Global sobre Ciberdelincuencia". *Proxyrack*, 12 de octubre de 2023, www.proxyrack.com/blog/global-cybercrime-report/.
[cliv] "Informe Global sobre Ciberdelincuencia". (2023).
[clv] Shank, Stefanie. "El Informe Global de Ciberdelincuencia 2023: Una mirada a las conclusiones clave".

DIGI AMERICAS ALLIANCE MEMBERS

INFORME LATAM CISO 2024

DIGI AMERICAS LATAM CISO

Duke UNIVERSITY