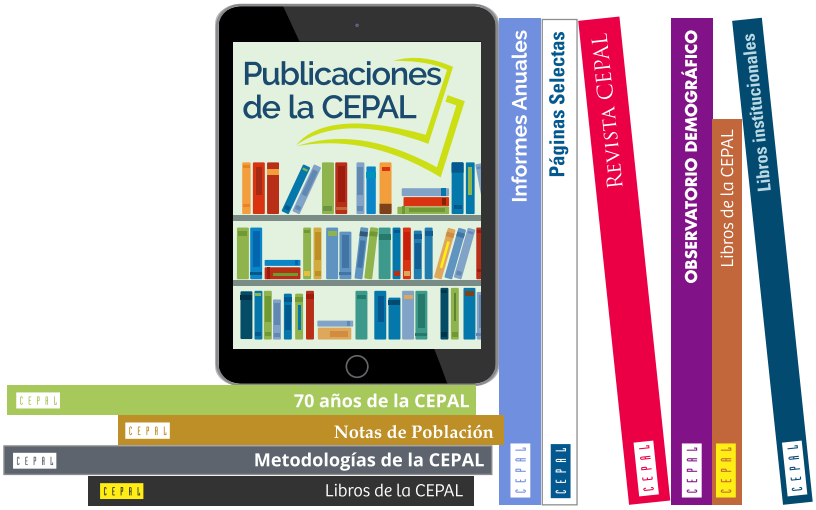
Ciberataques a la logística y la infraestructura crítica en América Latina y el Caribe

Rodrigo Mariano Díaz
Georgina Núñez

Naciones Unidas
CEPAL
75 años
Trabajando por un futuro productivo, inclusivo y sostenible
e
DESARROLLO en transición
Instrumento regional de la Unión Europea para América Latina y el Caribe

Gracias por su interés en esta publicación de la CEPAL



Si desea recibir información oportuna sobre nuestros productos editoriales y actividades, le invitamos a registrarse. Podrá definir sus áreas de interés y acceder a nuestros productos en otros formatos.

Deseo registrarme

www.cepal.org/es/publications

www.instagram.com/publicacionesdelacepal

www.facebook.com/publicacionesdelacepal

www.issuu.com/publicacionescepal/stacks

www.cepal.org/es/publicaciones/apps

NACIONES UNIDAS

CEPAL

Documentos de Proyectos

Ciberataques a la logística y la infraestructura crítica en América Latina y el Caribe

Rodrigo Mariano Díaz
Georgina Núñez

NACIONES UNIDAS
CEPAL

DESARROLLO en transición
Instrumento regional de la Unión Europea

Este documento fue elaborado por Rodrigo Mariano Díaz, Consultor, y Georgina Núñez, Oficial de Asuntos Económicos, ambos de la División de Desarrollo Productivo y Empresarial de la Comisión Económica para América Latina y el Caribe (CEPAL).

Los autores agradecen los comentarios de David del Moral, Jefe de la Sección de Tecnologías de Información y Comunicaciones de la CEPAL.

Esta publicación contó con el apoyo del Mecanismo Regional para el Desarrollo en Transición de la Unión Europea, en el marco del proyecto "Observatorio regional de desarrollo digital" de la CEPAL y la Unión Europea.

Publicación de las Naciones Unidas
LC/TS.2023/93
Distribución: L

Impreso en Naciones Unidas, Santiago
S.23-00614

Esta publicación debe citarse como: R. M. Díaz y G. Núñez, "Ciberataques a la logística y la infraestructura crítica en América Latina y el Caribe", *Documentos de Proyectos* (LC/TS.2023/93), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2023.

Índice

Cuadros

Gráficos

Diagramas

Introducción

La acelerada digitalización producto de la mayor conectividad ha situado a las agendas digitales al centro de la política pública de los países. Así mismo se ha enfatizado la necesidad de incentivar a los distintos actores a alinear su comportamiento con las expectativas de protección de datos[1] y la ciberseguridad[2]. En casi todos los análisis ha estado presente la falta de herramientas y datos necesarios para una adecuada coordinación regional en dichos temas, a pesar de los esfuerzos desplegados a nivel internacional, regional y nacional por contener las múltiples amenazas desplegadas sobre las infraestructuras y los sectores económicos clave y disminuir las vulnerabilidades generadas.

La agenda digital de América Latina y el Caribe (ALC) junto a los cambios acelerados asociados a la cuarta revolución industrial ocupan un lugar de importancia central para la Comisión Económica para América Latina y el Caribe (CEPAL). Como parte de la continua preocupación por el incremento en los incidentes que afectan la seguridad cibernética de la región, desde el año 2020 la CEPAL realiza un seguimiento del estado de la ciberseguridad en la región (CEPAL, 2021).

En la región ha habido avances en el fortalecimiento de los marcos normativos de protección de datos y de seguridad cibernética. No todos los países de América Latina y el Caribe cuentan con herramientas regulatorias en materia de protección de datos y ciberseguridad. Según el Rastreador Global de Legislación Cibernética de la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD, por sus siglas en inglés), sólo 24 de los 33 países de América Latina y el Caribe tienen legislación sobre privacidad y protección de datos personales. En cuanto al tema de la seguridad de los datos, según el Índice de Ciberseguridad Global (ICG) de la Unión Internacional de Telecomunicaciones (UIT)[3] existen diferencias importantes entre los países de la región. Brasil lidera la

[1] https://repositorio.cepal.org/bitstream/handle/11362/44629/1/S1900395_en.pdf.

[2] https://repositorio.cepal.org/bitstream/handle/11362/45988/4/S2000552_en.pdf. https://www.cepal.org/es/publicaciones/47240-estado-la-ciberseguridad-la-logistica-america-latina-caribe.

[3] El GCI mide el nivel de ciberseguridad en 194 jurisdicciones basándose en cinco pilares: legislación, medidas técnicas, organizaciones, desarrollo de capacidades y cooperación.

clasificación con 96,6 puntos sobre 100, seguido de México, Uruguay y la República Dominicana (+75). En cambio, algunos países de Centroamérica y el Caribe tienen menos de 15 puntos[4].

A partir de la pandemia provocada por el coronavirus (COVID 19) se han hecho algunos avances legislativos. No obstante, estos no han sido trasladados a través de una posición única regional a una mesa de negociación multilateral. Europa, en cambio, ha podido regular en forma colectiva los temas digitales sin preocuparse mucho del impacto transfronterizo, a través, por ejemplo, de la Ley de Servicios Digitales, y la Ley de Mercados Digitales[5].

El presente estudio hace una recopilación de incidentes ocurridos en diez países seleccionados de América Latina (Argentina, Brasil, Chile, Colombia, Ecuador, México, Panamá, Perú, República Dominicana y Uruguay) como e informes publicados por instituciones referentes del sector de ciberseguridad entre 2020 y 2022, la cual se suma a la información obtenida de los Equipo de Respuesta a Incidentes de Seguridad.

Según la consultora internacional KPMG (2022), los riesgos actuales que generan mayor preocupación podrían verse como una "triple amenaza" formada por fraude, infracciones de cumplimiento y ciberataques. Solo el 19% de las instituciones en Latinoamérica cumple con al menos el 50% de los controles relacionados con la ciberseguridad (KPMG, 2022). Al mismo tiempo el informe señala que las pérdidas por un manejo inapropiado de la ciberseguridad ascienden al 1,5% de la facturación anual de las empresas lucrativas, sin considerar los costos intangibles que representan la pérdida de reputación en imagen.

De acuerdo con (Daugherty, P. R., 2018) el robo de información personal que se produce durante una violación de ciberseguridad erosiona la confianza de los clientes, inversores, empleados y otras partes interesadas, lo que evidencia el estrecho vínculo entre el riesgo cibernético y el riesgo social. Los nuevos requisitos de divulgación y presentación de informes incorporados en las últimas regulaciones de la Comisión de Seguridad e Intercambio que rigen la supervisión de la ciberseguridad subrayan el vínculo entre el riesgo de gobernanza y el riesgo cibernético. La ciberseguridad debería ser considerada como una parte importante de los análisis basados en factores ambientales, sociales y de gobernanza (ASG o ESG por sus siglas en inglés) en las empresas, las que están avanzado a ritmo acelerado, a pesar de que las organizaciones gubernamentales muestran un menor dinamismo en la materia (Mishra, 2022). La ciberseguridad ya ha sido incorporada a la matriz de riesgo de las empresas y la mayoría de las políticas de gestión de riesgos ya incluye en su análisis y supervisión del riesgo, puramente financiero a las áreas ESG, incluida la ciberseguridad. El riesgo cibernético puede ser tan perjudicial para la reputación y el valor de una empresa como cualquier otro problema de ESG, y el daño que se inflige impacta de igual manera a la operación y a estrategia empresarial, y, nuevamente, no se la advierte integrada a las estrategias de los países de modo generalizado. A medida que los ataques cibernéticos aumentan en tamaño y frecuencia, el daño directo e indirecto a las empresas, incluida la pérdida de confianza del cliente, el daño a la reputación, el impacto potencial en el precio de las acciones y las posibles acciones regulatorias o litigios, podría afectar a cada aspecto de la estrategia ESG.

Mientras el Foro Económico Mundial (2022)[6] coloca a los ciberataques en segundo lugar, inmediatamente después de los riegos de desastres naturales de la misma manera que lo hace RBC Global Asset Management, el único tema relacionado con la gobernanza en el ESG de mayor preocupación que la ciberseguridad, es el riesgo de anticorrupción.

---

[4] Global Cybersecurity index 2020. Unión Internacional de Telecomunicaciones (UIT), 2022. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.

[5] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en. https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFIN.

[6] https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf.

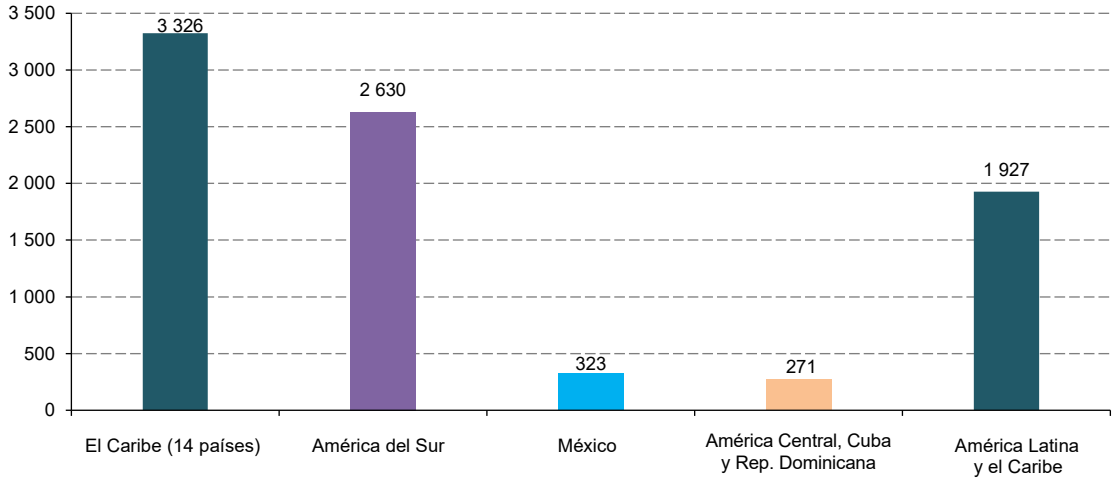
El presente estudio es producto de una investigación de escritorio, la cual incluye recopilación de incidentes ocurridos en América Latina y el Caribe e informes publicados por instituciones referentes del sector de ciberseguridad entre 2020 y 2022, sumado a información obtenida de los Equipo de Respuesta a Incidentes de Seguridad o *Cyber Security Incidents Response Team (CSIRT)* consultados.

En resumen, se lleva a cabo un informe que está estructurado en un marco de referencia, seguido de un capítulo de relevamiento de la situación regional y global de la ciberseguridad, posteriormente una propuesta de recomendaciones generales, y finaliza con un breve resumen, a modo de recopilación, aunando a las conclusiones y recomendaciones.

I. Relevamiento regional y global: marco de referencia

La privacidad y la seguridad cibernética son componentes clave de la digitalización y esenciales para la confianza. De acuerdo con el Banco Mundial (2022), en América Latina y el Caribe hay 1.928 servidores seguros por cada millón de personas. Aunque existen contrastes sustanciales entre Sudamérica y el Caribe en comparación con México y Centroamérica (véase el gráfico 1) todos los países de la región, excepto Belice, están por detrás de las economías desarrolladas (57.452 sitios en el conjunto de los miembros de la Organización para la Cooperación y Desarrollo Económico, OCDE).

Gráfico 1
Servidores de Internet seguros por millón de habitantes, 2020
(Número de certificados TLS/SSL distintos y de confianza pública encontrados en la Encuesta de Servidores Seguros de Netcraft)



Fuente: En base a The World Bank (2022) https://www.worldbank.org/en/topic/financialinclusion/overview#1.
Nota: Belice, Guyana y Surinam están incluidos en la región del Caribe.

Sin duda, la armonización de los marcos normativos/regulatorios de la región en materia de protección de datos y ciberseguridad podría crear importantes beneficios económicos y sociales que incrementen la confianza de los inversionistas extranjeros y nacionales y promuevan la innovación y la diversificación económica. La implementación de marcos normativos/regulatorios innovadores, como los entornos de pruebas regulatorias (regulatory sandboxes) contribuyen a fomentar mejores condiciones de mercado y un mayor crecimiento económico. Por su parte, la interoperabilidad tiende a estar determinada por las políticas públicas, esto es, los países no sólo deben fomentar la compatibilidad técnica y jurídica entre los distintos sistemas e incrementar la cooperación internacional para facilitar por ejemplo la transferencia transfronteriza de datos de forma segura. Los avances en acuerdos multilaterales que mejoren las operaciones transfronterizas seguras sin duda impactan positivamente la transformación digital de la región.

El llamado a la armonización de los marcos normativos y regulatorios se hace imperioso en un contexto que presenta a China como el primero de los 10 países con mayores pérdidas debido al cibercrimen en el año 2021, con un monto estimado en 574 mil millones de dólares, lista que alcanza 2 de los países de la región; Brasil en segundo lugar con 188 mil millones de dólares y México en noveno lugar con una cifra de u$s 31.600 millones según la firma IBM[7].

Los 27 millones de pequeñas y medianas empresas (PyMES) que existen según el Banco Interamericano de Desarrollo, representan un sector económico de gran impacto social y económico en América Latina y el Caribe. Según la firma dedicada a la ciberseguridad Kaspersky, las PyMES de la región pueden tener pérdidas de hasta u$s 155 mil al sufrir un ciberataque, además de enfrentar consecuencias como multas y compensaciones a clientes y autoridades, pérdidas de socios de negocio o daños a su imagen o reputación[8].

A. Eventos destacados en logística e infraestructuras críticas

A través de la investigación de escritorio realizada, se ha podido documentar un total de 82 incidentes que afectaron a los diez países investigados en el presente informe y que se detallan en el cuadro 1. En el se visualiza los siguientes datos estadísticos ocurridos entre 2020 y 2022.

Cuadro 1
Cantidad de incidentes encontrados por país

País	Cantidad	Porcentaje
Brasil	27	19
Colombia	20	14
Argentina	19	13
Chile	16	11
México	15	10
Perú	11	8
Uruguay	11	8
Ecuador	10	7
República Dominicana	8	6
Panamá	7	5

Fuente: Elaboración propia.

[7] https://es.scribd.com/document/637504392/study-id128160-digital-economy-compass-2022#.
[8] https://latam.kaspersky.com/blog/pymes-latam-enfrentan-creciente-numero-ciberataques/24950/.

Al mismo tiempo, categorizados según la triada de seguridad definida en la norma internacional ISO/IEC 27001 (ISO/IEC, 2022), se contabilizaron 54 incidentes que afectaron la disponibilidad, 74 la confidencialidad y 25 la integridad. Si bien, del total de los ataques registrados, la mayoría de aquellos relevados corresponden a afectaciones de tipo *ransomware* —consistentes en un cifrado de datos en el que se pide un pago por su "rescate"—, aún se percibe un bajo nivel de compromiso de las instituciones con la denuncia de los respectivos incidentes acontecidos. En la sección "Ciberseguridad en América Latina y el Caribe y su relación con las instituciones públicas" el tema se analiza en detalle.

Al estudiar el impacto en el primer vertical, **"disponibilidad"**, se encuentra que tan solo en 26 de los incidentes ocurridos (32%) se han evaluado e informado el tiempo del impacto, llegando a ser de un 1 día en los casos más leves, mientras que, en los casos más complejos, toma hasta 540 días retomar la normalidad. El promedio de 54 días es el tiempo que tarda una institución en lograr la recuperación del total de los procesos internos asistidos por la tecnología afectada.

Si se observa el impacto desde el punto de vista económico se puede ver que tan solo 11 casos (el 13% de los eventos inventariados) cuentan con esta información; gracias a ello, se pudo investigar los costos de las brechas de seguridad sufridas. Esta información conforma un conjunto importante de datos reales, ya que hay ocasiones en que realizar un coste cuantitativo de las pérdidas es una tarea altamente difícil. Además, se debe considerar que los valores informados no contemplan una cuantificación económica por la pérdida de reputación e imagen de la institución afectada. Estos valores parten de los US$ 4200 y pueden llegar a valores de hasta US$ 570 millones esto es, un promedio de US$56 millones de dólares. El total de las pérdidas económicas debido a todos los eventos inventariados asciende en América Latina y el Caribe a US$ 622.166.200. En el anexo 1 de incidentes podrán consultarse los detalles de este apartado.

Cuadro 2
Resumen de Inventario de Incidentes en América Latina y el Caribe

Cantidad de Incidentes		82	
Afectaron	Disponibilidad	54	66%
	Confidencialidad	74	90%
	Integridad	25	30%

Fuente: Elaboración propia.

Desde el relevamiento regional realizado, a través de la Unidad de Inversiones y Estrategias Empresariales, se hizo la consulta a los CSIRT de los países considerados en el presente estudio, a través de las direcciones de correo electrónico disponibles en sus páginas institucionales, fue posible obtener información relevante sobre incidentes entre 2020 y 2021, véase el anexo 2. Cabe mencionar que se obtuvo una respuesta inmediata del CSIRT del Gobierno de la Ciudad de Buenos Aires, Argentina y también del mismo organismo de nivel nacional de Panamá, Chile y Brasil. El primero de ellos, reportó los datos contenidos en el gráfico 1. Entre mayo 2021 y mayo 2022 se registró el mayor incremento de denuncias, seguido por el período noviembre 2020-noviembre 2021. Mientras que, los períodos con menor incremento fueron enero 2021-enero 2022, octubre 2021-octubre 2022 y agosto 2021-agosto 2022.

El mismo centro de la Ciudad Autónoma de Buenos Aires informó el siguiente ranking por tipo de incidente:

i) Fraude/estafa derivada de transacción online (21%)

ii) Ingeniería social (11,5%)

iii) Phishing (9,7%). *Si bien el phishing es una técnica considerara dentro de la ingeniería social, se distingue por la cantidad de sitios web fraudulentos reportados que no siempre califican —únicamente— como ingeniería social*

iv) Fraude derivado de uso ilegítimo de credenciales y/o acceso indebido en cuentas online (8%)

v) Suplantación de identidad digital (6,5%). *Cuando la suplantación de identidad digital se produce derivada de un previo acceso indebido, prima dicho incidente y se categoriza como "acceso indebido a cuenta online"*

vi) Acoso y/u hostigamiento digital (4%)

vii) Compromiso de cuenta de usuario (1,8%)

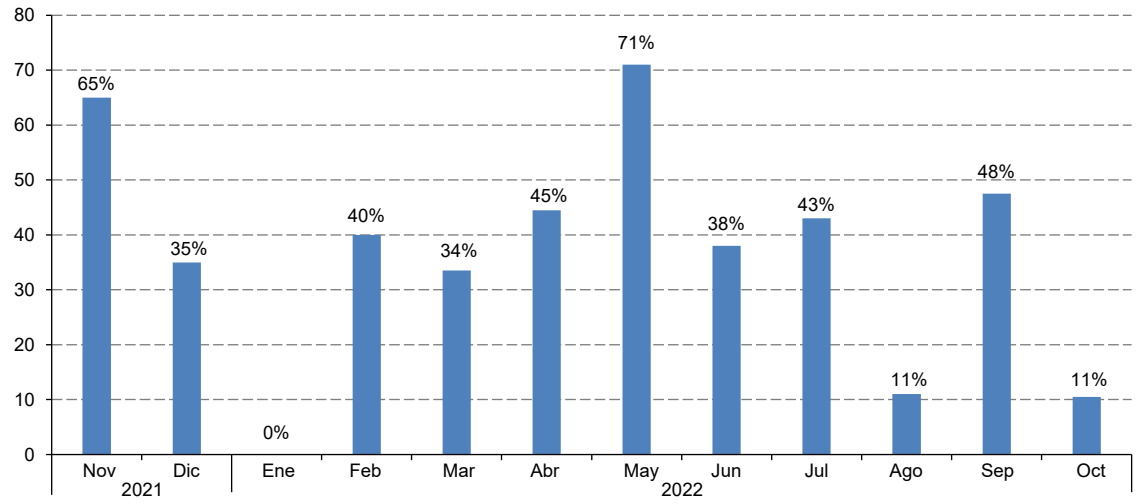
viii) Publicación no autorizada de información (1,5%)

ix) Violencia de género digital (1,5%)

x) Sextorsión (1%). Estás dos últimas *categorías suelen presentarse acompañadas de acoso y/u hostigamiento digital (incluso, a veces, amenazas) y suele añadirse difusión sin consentimiento de material audiovisual íntimo.*

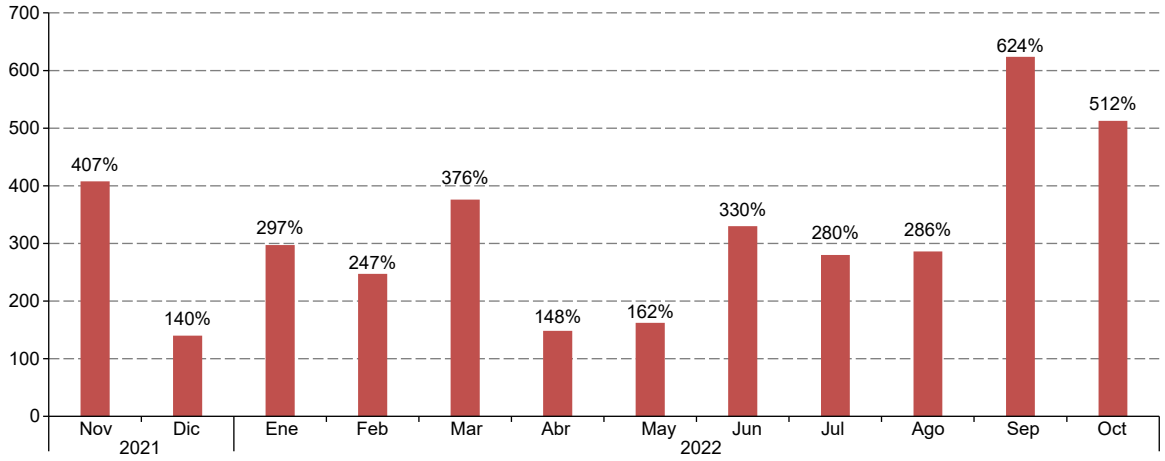
Por su parte, el CSIRT de Panamá informó los datos incluidos en el gráfico 2, en el cual se observa que el mayor incremento se produjo entre septiembre 2021 y 2022, siendo diciembre y abril los meses con menor crecimiento interanual.

Gráfico 2
Crecimiento interanual de incidentes según denuncias recibidas por CSIRT Ciudad Autónoma de Buenos Aires 2022



Fuente: Elaboración propia con datos provistos por el CSIRT de la Ciudad Auntónoma.

Gráfico 3
Crecimiento interanual de incidentes según denuncias recibidas por CSIRT Panamá 2022

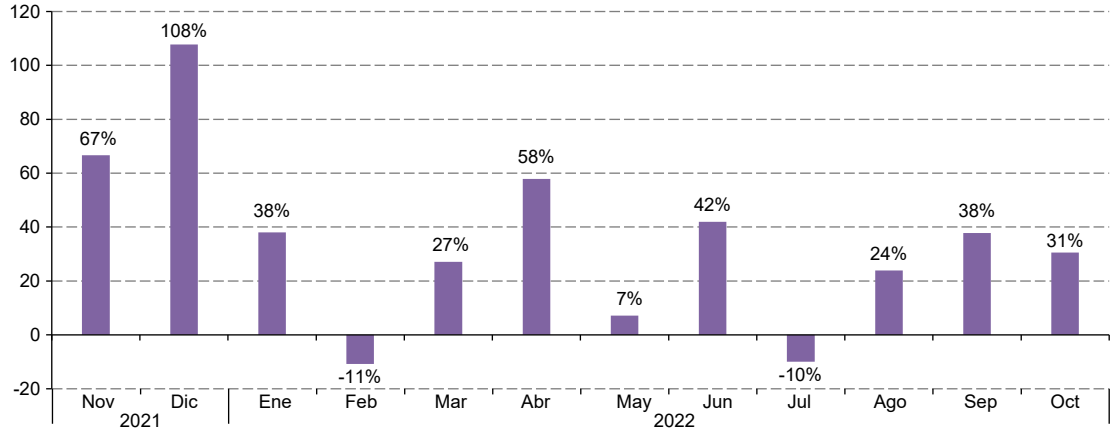


Fuente: Elaboración propia con datos provistos por el CSIRT del Gobierno de Panamá.

Al mismo tiempo, el organismo panameño detalla un promedio mensual de 295 denuncias recibidas con un valor máximo de 426 en el mes de mayo de 2022.

La información compartida por CSIRT del Gobierno de Chile representada en el gráfico 4, observa el mayor crecimiento interanual en el mes de diciembre de 2021. En febrero y en julio de 2022 se observa un descenso respecto al mismo mes del año anterior. Dentro de la totalidad de los incidentes atendidos, 76% correspondieron a algún tipo de vulnerabilidad, 10% a incidentes que afectaron la disponibilidad de las instituciones atacadas y el 14% restante a otras afectaciones, entre las cuales el fraude ocupa el primer lugar con un porcentaje de 5%. Es importante destacar que durante el año 2022, la institución recibió denuncias por 35 ataques a instituciones con un impacto elevado, es decir que en Chile existe un incidente de ciberseguridad con impacto grave cada 10,4 días.

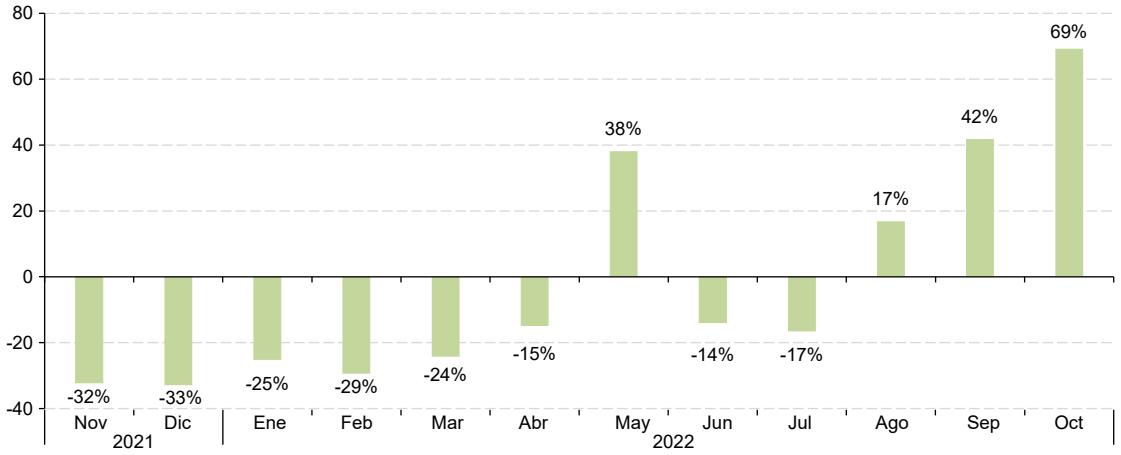
Gráfico 4
Crecimiento interanual de incidentes según denuncias recibidas por el CSIRT Chile 2022



Fuente: Elaboración propia con datos provistos por el CSIRT del Gobierno de Chile.

Los datos obtenidos del CSIRT del Gobierno de Brasil está representada en el gráfico 5, y se observa el mayor crecimiento interanual en el mes de octubre de 2022. En los meses que van desde noviembre de 2021 hasta julio de 2022 se aprecia un descenso respecto al mismo mes del año anterior excepto en el mes de mayo 2022 donde se registra un crecimiento del 38%. Dentro de la totalidad de los incidentes atendidos, 72% correspondieron a escaneos, 14% a incidentes que afectaron la disponibilidad de las instituciones atacadas y el 14% restante a otras afectaciones, entre las cuales el fraude ocupa el primer lugar, de la misma manera que ocurrió en Chile, pero en este caso con un porcentaje de 7%.

Gráfico 5
Crecimiento interanual de incidentes según denuncias recibidas por el CSIRT Brasil 2022



Fuente: Elaboración propia con datos provistos por el CSIRT del Gobierno de Brasil.

El equipo de respuesta a incidentes de Chile ha atendido un promedio de 2199 incidentes por mes, con un máximo de 2602 en el mes de mayo de 2022, coincidente con el mismo período de mayor actividad informado por Panamá. La cifra promedio en Brasil de denuncias mensuales ascendió a 38.420 siendo mayo el segundo mes de mayor actividad, ya que, en el caso de Brasil, el mes de agosto resultó el mes con mayor actividad declarada.

Cuadro 3
Cantidad de eventos mensuales recibidos en denuncias por los CSIRT

Mes	Panamá	Chile	Brasil
Noviembre 2021	110	2 036	31 329
Diciembre 2021	88	2 360	26 349
Enero 2022	211	1 569	33 477
Febrero 2022	235	1 509	27 472
Marzo 2022	342	2 492	37 553
Abril 2022	255	2 482	28 351
Mayo 2022	426	2 602	50 437
Junio 2022	353	2 261	35 706
Julio 2022	294	2 107	34 098
Agosto 2022	392	2 474	62 695
Septiembre 2022	424	2 073	45 396
Octubre 2022	415	2 420	48 178
Promedio	295	2 199	38 420

Fuente: Elaboración propia con datos provistos por los CSIRT del Gobierno de Chile, Panamá y Brasil.

B. La realidad de América Latina dentro del contexto mundial

Las distintas organizaciones que realizan trabajos atendiendo las cuestiones de seguridad informática aplicando soluciones globalizadas, afirman que, en el transcurso del tercer trimestre del año 2022, cada organización recibió en promedio un total de 1130 ataques por semana, lo cual representa un crecimiento interanual del 28% (Checkpoint, 2022). Si se considera el total acumulado durante los dos años analizados, los ataques crecieron hasta un 59% con respecto a la información registrada en el informe 2021 de CEPAL. El reporte elaborado por la firma Checkpoint se realiza con la información recolectada por los sistemas de prevención que se encuentran desplegados a nivel mundial. La actividad detectada por las protecciones perimetrales de la red se concentra en sistemas centralizados los cuales son los encargados de realizar las tareas de procesamiento, determinar nuevos patrones y redistribuir las distintas actualizaciones en los modelos de protección a los equipos y productos de sus clientes.

Este mismo estudio señala que Latinoamérica ocupa el segundo lugar en cantidad de ataques por institución y el tercero en crecimiento interanual de ataques a nivel global.

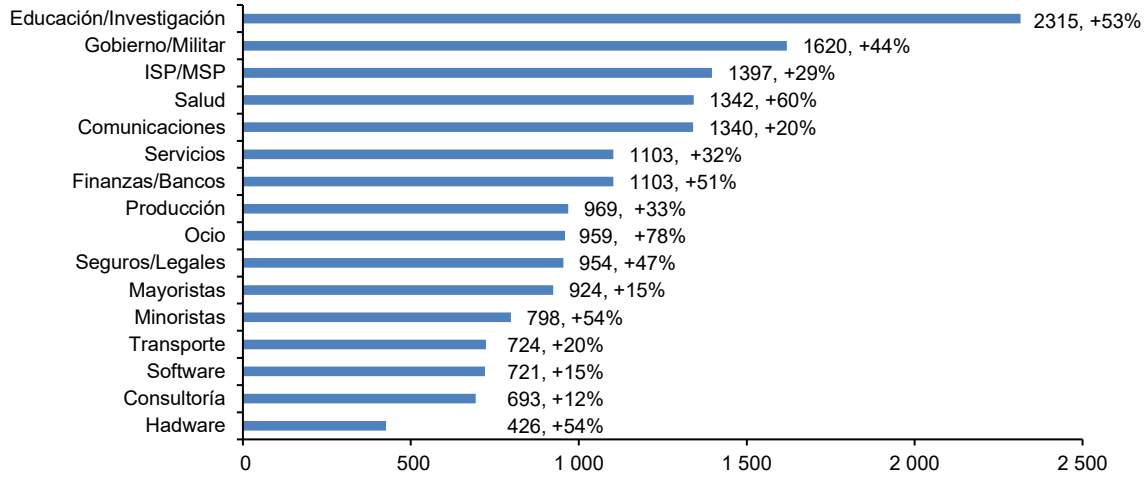
Cuadro 4
Cantidad de ataques semanales por región

Región	Ataques por semana	Cambio Interanual
ANZ	904	72%
América del Norte	849	47%
América Latina	1 572	32%
Europa	896	22%
Asia	1 778	21%
África	1 549	-6%

Fuente: Checkpoint, 2022.

De acuerdo con datos recolectados por Checkpoint (2022), el sector que más ataques recibe es el de educación e investigación, seguido del sector gubernamental y, por último, el de salud, siendo estos últimos sectores quienes han ocupado los dos primeros lugares de manera sostenida a lo largo del tiempo. Sin embargo, el sector de ventas masivas es el que denuncia el mayor crecimiento interanual en ataques, alcanzando un 69%, seguido de salud con un 60%, y en tercer lugar el sector de finanzas con un crecimiento interanual de 40%.

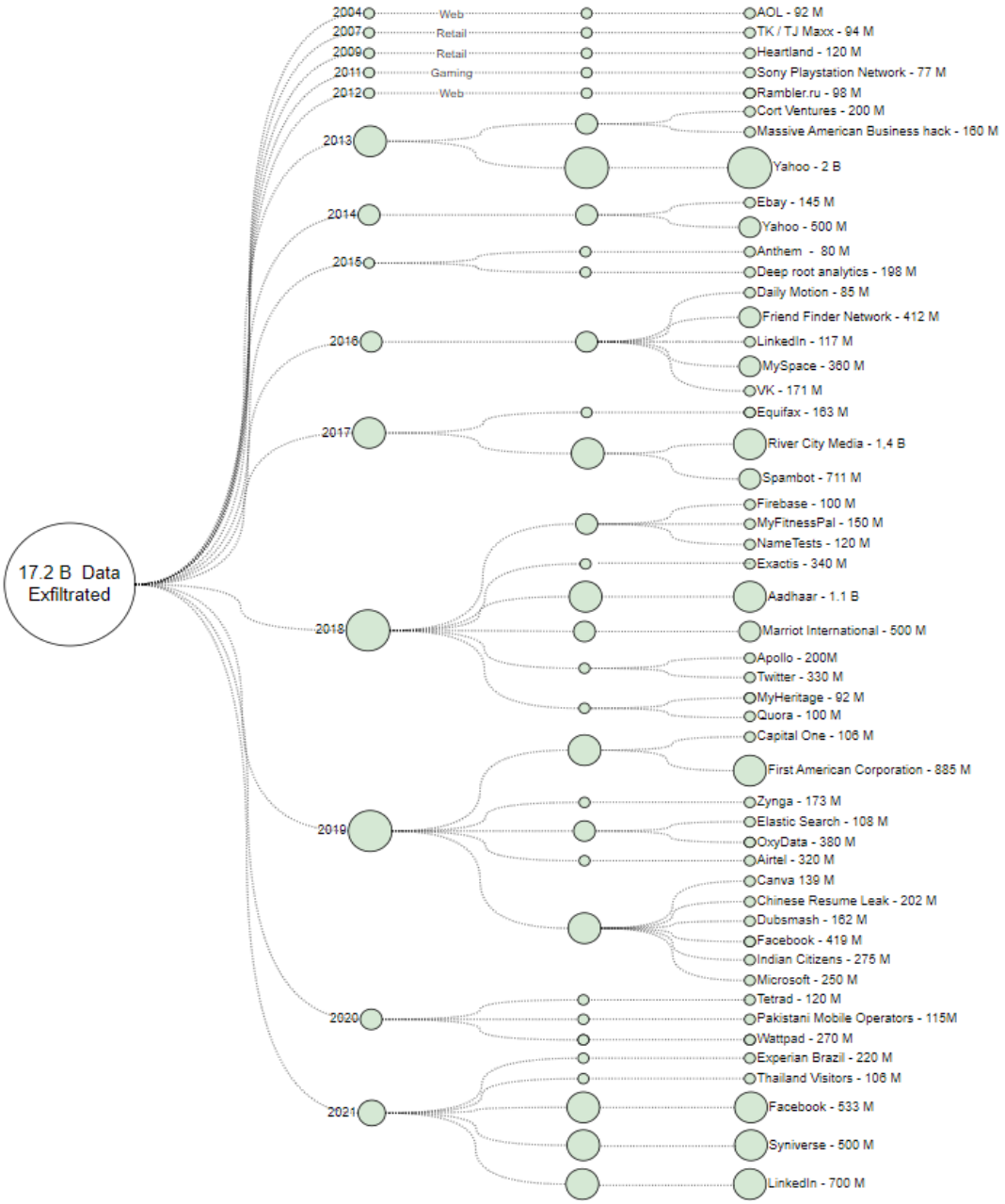
Grafico 6
Promedio semanal por organización por industria – global tercer trimestre 2022



Fuente: Checkpoint, 2022.

Otros estudios recientes en el área de la ciberseguridad confirman que los ciberatacantes capturan aproximadamente 95 contraseñas de acceso por segundo. Mientras que, en el transcurso del año, son más de tres mil millones las cuentas de usuarios robadas con sus respectivas claves de acceso, generalmente obtenidas a través de exfiltraciones generadas por brechas de seguridad o algún tipo de programa maligno o *malware* (Pawar, 2022). Estos estudios indican también que solo el 20% de los usuarios toman la medida de cambiar sus contraseñas luego de enterarse que sus credenciales han sido comprometidas. Esta realidad es de especial importancia en posibles acciones a futuro, sobre todo si se tiene en cuenta la gran cantidad de registros que se exponen a internet de manera incesante año tras año.

Diagrama 1
Histograma filtración de datos



Fuente: Gartner, 2021.

A la hora de verificar las estadísticas que afectan específicamente a las redes operacionales, es decir, aquellas que de manera exclusiva se utilizan para gestionar plataformas operativas en las cuales se alojan los sistemas SCADAS[9] encargados de comandar y controlar los PLC[10] (responsables del control de los procesos productivos en las instalaciones industriales), se puede visualizar y concluir que, del total estudiado, menos del 20% de las empresas cumplen con la premisa mínima, que es la de un inventario de activos adecuado en características y frecuencia de ejecución. Además, aquellas empresas que realizan un plan efectivo para la actualización de la gestión de su plataforma operativa se encuentran por debajo del 33% de las estudiadas. Sin embargo, lo que resulta aún más preocupante es que para esa misma proporción de organizaciones, la ciberseguridad de este tipo de instalaciones es un punto ciego en las áreas de altos mandos y de dirección, principalmente por una falta de actualización paradigmática respecto al aislamiento de las redes operacionales. Esto sin mencionar que más del 67% no está pensando realmente en tomar acciones de ciberseguridad relacionada con dichas instalaciones (Rockwell Automation Inc., 2022).

Un informe reciente emitido por Waterfalll, empresa dedicada a la seguridad de redes operacionales, indica que durante 2021 existieron 64 incidentes con pérdidas operativas mayores, representando un crecimiento del 144% respecto a 2020 (Ginter & Hale, 2021). Entre ellos se encuentra el ataque en mayo de 2021 a Colonial Pipeline, que debió detener por seis días el oleoducto este de Estados Unidos. El 18% de los incidentes mayores inventariados en dicho informe, corresponde al área de transporte, involucrando infraestructura de puertos y operaciones marítimas.

El comercio transnacional de mercancías, y su transporte, dependen en gran medida del desempeño de los sectores portuario y marítimo, el que alcanza mayor eficiencia cuanto más eficaces resultan los mecanismos de facilitación del comercio que reduzcan el tiempo y los costos de los trámites aduaneros y mercantiles e integren las nuevas tecnologías en las formalidades administrativas. Esto mejora el desempeño de toda la cadena de suministro y tiene efectos positivos para el transporte marítimo, destrabando las barreras burocráticas y acelerando los procedimientos de despacho.

Los mares y las vías navegables interiores son clave para el desarrollo económico presente y futuro y para la prosperidad de todas las naciones. La OCDE pronostica que el volumen del comercio marítimo se triplicará hasta 2050, lo que implica la necesidad de articular sistemas de comunicación abiertos, protegidos y seguros, que, junto con una buena gobernanza marítima y portuaria, basada en normas internacionales, resulten fundamentales para la seguridad y la prosperidad a escala mundial. Estas necesidades representan un desafío importante en la actualización de los estándares de comunicaciones utilizados, ya que históricamente se utilizaron sistemas de comunicaciones de radio VHF que fueron evolucionando a medida que incorporaban nuevos servicios, como por ejemplo *AIS* y los sistemas asociados. También la señalización ayuda a la navegación en su versión actual digitalizada, empero claro requieren revisiones asociadas a la confidencialidad e integridad de las comunicaciones inalámbricas.

Ya en febrero de 2019, un gran buque portacontenedores que navegaba hacia Nueva York identificó una intrusión cibernética a bordo que sorprendió a la Guardia Costera de los Estados Unidos[11]. Aunque el ataque de un malware[12] nunca controló el movimiento del buque, las autoridades concluyeron que las defensas débiles exponían funciones críticas a "vulnerabilidades significativas". En

---

9 Los sistemas de control y adquisición de datos (SCADA) se utilizan para controlar, supervisar y analizar los dispositivos y procesos industriales. El sistema consta de componentes de software y hardware y permite la recopilación remota e in situ de datos de los equipos industriales. Fuente: https://scada-international.com/es/what-is-scada/.

10 Un Control Lógico Programable (PLC) básicamente es una especie de computadora que se utiliza para realizar tareas automatizadas, como pueden ser líneas de ensamblaje en fábricas, sistemas de iluminación o cualquier otro tipo de proceso que sea automatizable. Fuente: https://bricos.com/noticias/que-es-un-plc-control-logico-programable/.

11 https://news.sophos.com/es-es/2019/07/12/un-ciberataque-lleva-a-un-barco-a-aguas-turbulentas/.

12 Malware, o software malicioso, es un término general para cualquier tipo de software con intenciones maliciosas. La mayoría de las amenazas online son algún tipo de malware. Fuente: https://es.malwarebytes.com/malware/.

esa oportunidad no ocurrió un desastre marítimo, pero se encendió una severa llamada de advertencia sobre una amenaza emergente para el comercio mundial: la piratería cibernética era capaz de penetrar la tecnología a bordo que se encontraba reemplazando las viejas formas de dirección, propulsión, navegación y otras operaciones clave. Tales saltos en las capacidades de piratería podrían causar, en primer lugar, un enorme daño humano, con el consecuente perjuicio económico.

Según Wayne Arguin, comandante asistente de la Guardia Costera de los Estados Unidos para la política de prevención, el transporte marítimo enfrenta riesgos cibernéticos similares a los de otras industrias, solo que lo que está en juego es mucho más dado que casi el 80% del comercio mundial se mueve en el mar. Si bien Arguin no precisó un número en la frecuencia de los intentos de robo, dijo: "Me siento muy seguro de que todos los días se están probando las redes, lo que realmente refuerza la necesidad de tener un plan" (EEUU, 2022).

Este contexto engloba la actividad específica del transporte marítimo de pasajeros, siendo los cruceros un objetivo potencial de mayor interés para la piratería informática, debido al nivel de vulnerabilidad al que queda expuesta la víctima de este tipo de ataques.

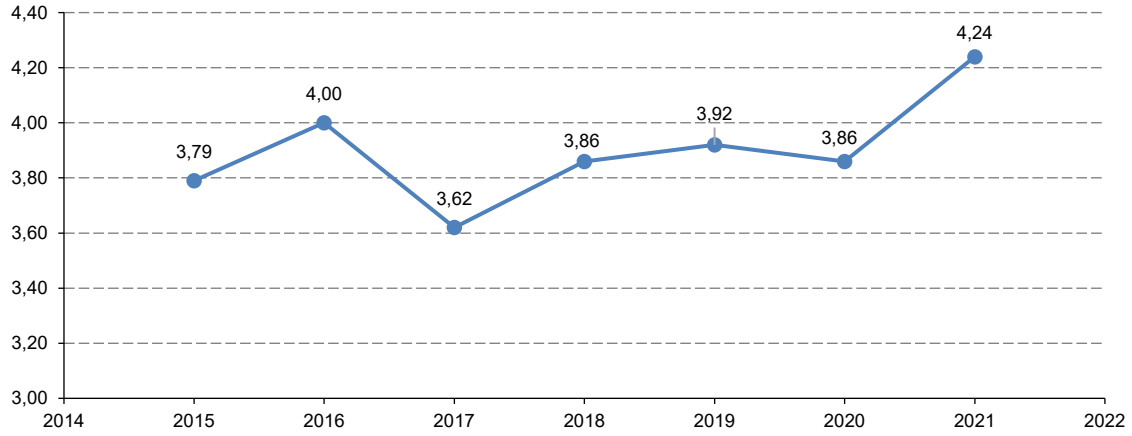
Algunos sucesos que han marcado la historia de la industria marítima entre los años 2010 y 2021, se refieren a más de veinte acontecimientos, de los cuales solo dos fueron denunciados, que involucran a organizaciones de cruceros turísticos, en ambos casos el operador de cruceros Carnival Corporation & plc, por ataques ransomware en 2019 y 2020. En ambos casos información confidencial de los clientes, como los datos de las tarjetas de crédito, fue robada. La empresa recibió múltiples reclamos por el ataque.

Un reciente informe sobre ciberseguridad en viajes y turismo destaca la creciente demanda de productos y servicios de ciberseguridad por parte de las empresas de este rubro para lograr proteger los datos personales de sus clientes. Se estima que frente a los US$1400 millones invertidos en esta área durante el año 2021, para el 2025 dicha cifra ascenderá a US$ 2100 millones (Cruceros, 2022).

Según el Foro Económico Mundial (2022), alcanza el 95% los problemas de ciberseguridad atribuidos a errores humanos, los que podrían reducirse adquiriendo habilidades básicas como, por ejemplo, el uso de contraseñas seguras, la identificación de estafas de phishing, la comprensión de cómo se recopilan los datos y el cómo se rastrea una identidad digital en línea (Mee & Brandenburg, 2020). Estas afirmaciones surgen de distintas fuentes estadísticas que indican que el 85% de las infecciones siguen utilizando algún tipo de ingeniería social para lograr derribar la primera barrera de ingreso a la infraestructura atacada (Carlson, 2021).Se sabe que más del 66% de las instituciones exponen sus archivos sensibles a una porción de su dotación superior a 1.000 funcionarios. También se conoce que están por encima del 60% aquellas instituciones que poseen más de 500 contraseñas que pueden ser utilizadas indefinidamente, es decir, que no poseen fecha de vencimiento en la que deban cambiar o quedar inutilizadas (Varonis, 2021).

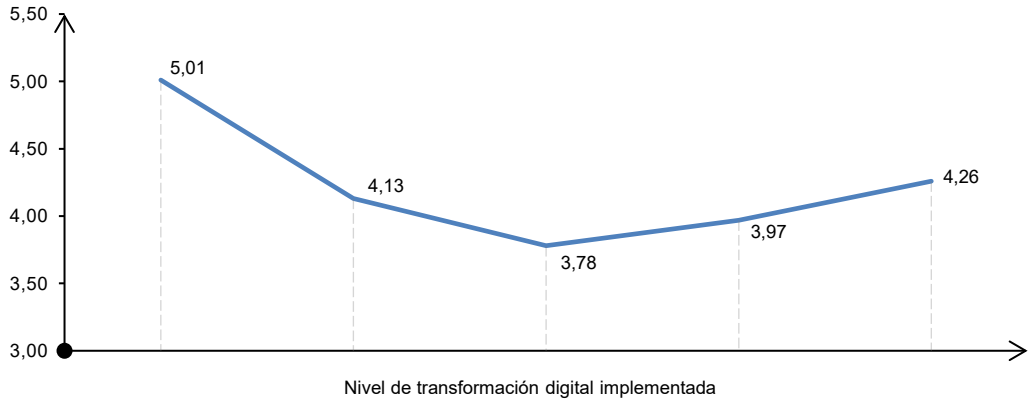
Según un reciente informe elaborado por la CEPAL, los rescates solicitados en un ataque de ransomware durante el segundo trimestre del año 2021 han promediado la suma de u$s 136.576, habiendo pasado por un pico de u$s 230.000 en el tercer trimestre del año anterior. Lejos quedan estos valores de los costos reales que dejan los incidentes, ya que se ha determinado que el promedio de tiempo con operaciones detenidas luego de un ataque de ransomware es de 23 días para 2021, cifras menores a 2020, donde la misma medición ascendía a 41 días. El mismo trabajo concluye sobre la base de información obtenida de IBM, que el costo total de las brechas de seguridad ascendió en promedio a 4.24 millones de dólares, es decir un 9.8% más que el costo promedio de 3.86 millones de dólares calculado para 2019. Particularmente en el sector de logística, este promedio ha sido de 3.75 millones de dólares para 2021 (Díaz, 2022). En el mismo informe se destaca que los costos de las brechas de seguridad han sido más elevados en las organizaciones que aún no han comenzado un proceso de transformación digital frente a aquellas que se han transformado por completo.

Gráfico 7
Costo promedio total de una brecha de seguridad
(En millones de dólares)



Fuente: Elaboración propia basada en datos de IBM Inc.

Gráfico 8
Costo de las brechas de seguridad versus nivel de transformación digital implementada
(En millones de dólares)



Fuente: Elaboración propia basada en datos de IBM Inc.

En un ataque de ransomware, el monto del rescate solicitado por los datos secuestrados está configurado por dos causas ya que, por un lado, se pone en riesgo la divulgación de información de valor elevado para la víctima, y por otro, el tiempo que la institución afectada necesita para volver a operar normalmente (CEPAL, 2021). El promedio de las recompensas solicitadas presentó un mayor crecimiento en el período 2020-2022, donde casos como el de Colonial Pipeline Co. y JBS Foods (HIPAA Journal, 2021) negociaron un rescate con la expectativa de evitar que la información secuestrada fuera divulgada. La confidencialidad de los datos comienza a posicionarse en un nuevo escenario para protegerse de los ataques, sobre todo considerando la obligatoriedad del cumplimiento de la regulación europea sobre protección de datos conocida por sus siglas GDPR para todos aquellos actuantes que administren datos personales de ciudadanos europeos, sin importar donde radique el actuante. Sumado a ello, la mayor parte de los países de América Latina y el Caribe ha firmado el convenio de Budapest, en donde se comprometen a colaborar con el proceso legal asociado a todo tipo de delito cibernético relacionado con la actividad en internet.

Ante este escenario, es preciso mencionar la dificultad de mantenerse en cumplimiento con estos términos si las estrategias de defensa no son modificadas y se mantienen sobre la línea actual. Según Gartner, para el fin del año 2023 las leyes de protección de datos personales alcanzarán al 75% de la población del planeta, en un esfuerzo global por atender a la confidencialidad, como la principal amenaza a la que se enfrenta la ciberseguridad. Un reciente informe de la mencionada consultora asegura que para el año 2025, el 60% de las organizaciones consideran su análisis de riesgo cibernético como la principal herramienta para realizar alianzas comerciales y transaccionar con terceros. Para atender apropiadamente este desafío será necesario que, para ese momento, el 40% de las juntas directivas cuenten con un comité especializado en ciberseguridad supervisado de manera directa por el directorio (Gartner, 2021).

El sector salud deberá atender esta necesidad especialmente por la particular importancia de los efectos y consecuencias que podrían llegar a generar la pérdida de confidencialidad de los datos bajo su custodia y demandas asociadas, todo esto por encima del grave problema que representa actualmente para sus servicios la pérdida de la disponibilidad, que ha llegado a causar efectos que van más allá de lo económico, informando dos incidentes mayores a los cuales se les podría atribuir la pérdida de vidas humanas en Estados Unidos de América (HIPAA Journal, 2021) y en Alemania (Pastor, 2020) como consecuencia de ciberataques.

Al rastrear a los grupos de atacantes en el ciberespacio, los organismos públicos internacionales y nacionales como Interpol y todas las divisiones de las fuerzas policiales alineadas, se encuentran con la dificultad de una escasa regulación internacional, y en muchos casos una falta de regulación local, que podría verse disminuida mediante las regulaciones que alcancen el movimiento de las monetizaciones que se generan ante los incidentes. De esta manera, regular el movimiento de divisas a través del uso de criptomonedas tendría un doble efecto positivo: i) acelerar algunos procesos ya digitalizados y su automatización en los pagos mediante el uso de contratos inteligentes, y también ii) la posibilidad de contar con mayor trazabilidad de la transacción de manera que sea posible llegar a los grupos de ciberataques por esta vía. Se estima que el porcentaje de estados nacionales que aprueban una legislación para regular los pagos, multas y negociaciones de ransomware aumentará 30% para fines de 2025, en comparación con menos del 1% en el 2021 (Gartner, 2021). Un claro ejemplo de estos cambios es el proyecto de ley de Estados Unidos de América, presentado el 5 de octubre de 2021, en donde se especifica que toda institución que realice un pago por rescate de un ransomware deberá denunciarlo al Departamento de Seguridad Nacional *(Department of Homeland Security-DHS)* dentro de las 48 hrs. de efectuado el pago (HIPAA Journal, 2021).

C. Mirar hacia el futuro junto a Costa Rica

El gobierno de Costa Rica ha declarado estado de emergencia ante un escenario de recurrentes ciberataques, o de "ciberguerra" tal como la misma entidad lo ha definido. La decisión fue en respuesta a los hechos técnicos ocurridos el 18 de abril de 2022, en que el grupo de atacantes Conti, con actividad detectada en Rusia, atacó múltiples instituciones públicas como por ejemplo al Ministerio de Trabajo, al de Ciencia, Tecnología y Telecomunicaciones, al Seguro Social y al Instituto Meteorológico Nacional; pero ha sido el Ministerio de Hacienda el que se ha visto más afectado, dejando sin utilidad la totalidad de los sistemas aduaneros (Amerise, 2022). Este evento deja un precedente en la región ya que, a pesar de ser de público conocimiento el esfuerzo institucional que toda la región viene realizando en materia de ciberseguridad, es el primer país en declarar estado de emergencia por hechos relacionados con el ciberdelito. Según la información recolectada por el diario La República en las instituciones privadas y principales exportadores, las pérdidas por la caída de los sistemas de Aduana se calculó en U$D 38 millones por cada día en el que los sistemas estuvieron fuera de servicio (Gutiérrez, 2022).

Es preciso señalar que Costa Rica ha adoptado una estrategia de digitalización de los servicios de exportación para fortalecerse económicamente en la región, y que en 2017 el gobierno costarricense determinó de manera oficial una Estrategia Nacional de Ciberseguridad, en donde se redactó un protocolo que incluye una serie de medidas para proteger a la nación de los ataques cibernéticos. Sin embargo, dicho plan contiene aún puntos de mejora y su implementación requiere alcanzar una mejor planificación con el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), al mismo tiempo que una mayor coordinación con el Equipo de Respuesta a Incidentes de Seguridad Cibernética (CSIRT) para monitorear y mitigar las posibles acciones que atenten contra el éxito de la estrategia de digitalización del estado.

Si se observa el grado de madurez en ciberseguridad que presentan los países de la región que se revisan en el presente informe, según el Observatorio de Ciberseguridad del Banco Interamericano de Desarrollo (BID) y la Organización de Estados Americanos (OEA), la situación de Costa Rica podría ser similar a la de aquellos países de este informe (BID y OEA, 2020). Se debería llamar a todos a replantear y revisar la manera en que se está llevando adelante las estrategias de prevención, recordando que la mejor acción sobre los hechos y pérdidas ocurridas, es la reflexión sobre lecciones aprendidas para lograr una mejor protección hacia el futuro, sobre todo y teniendo en cuenta que para pasar a la acción, cuando de tecnologías exponenciales se trata, "el mejor momento era el año pasado, y el segundo mejor momento es ahora" (Godin, 2014).

D. Ciberseguridad en América Latina y el Caribe y su relación con las instituciones públicas

En la versión publicada en 2021 sobre el Estado de la Ciberseguridad en América Latina y el Caribe (CEPAL, 2021) se presentó el estado de madurez de la ciberseguridad en diez países de la región (Argentina, Brasil, Chile, Colombia, Ecuador, México, Panamá, Perú, República Dominicana y Uruguay). Si bien la investigación arroja un importante proceso de concientización sobre la ciberseguridad, y aunque ocupa un lugar importante de preocupación en los países, aún es muy baja o nula, la actividad de actualización normativa y regulatoria es muy baja en aquellos documentados. De los países estudiados, solo Colombia muestra avances efectivos sólidos, al contar con cinco nuevos decretos nacionales, llegando así a fortalecer su posicionamiento en la región en materia de gobernanza digital. También Chile presenta una actualización importante a través de la ley 21.459, la cual es una modificación de la anterior (19.233), en la que se actualizan los cuerpos legales en relación con la adhesión del Convenio de Budapest. Ecuador por su parte ha dado un gran paso fijando una estrategia nacional de ciberseguridad a través del Oficio nº MINTEL-MINTEL-2022-0975-O-09082022 (Informática Jurídica, 2022).

Es preciso recordar los estados de madurez de cada uno de los países según el Observatorio de Ciberseguridad del BID-OEA presentados en el informe de 2020 (BID y OEA, 2020) que posiciona a cada país analizado en un grado de madurez de entre 1 y 5 de gobernanza cibernética.

En el anexo 2, se incluye la totalidad de las leyes relevadas actualmente vigentes y se detallan si son anteriores o posteriores al año 2020.

Se observa una amplia necesidad en toda la región por hacer un esfuerzo extra para acompañar a las instituciones del ámbito tanto público como privado con normativas y leyes que sean actualizadas y oportunas, en las que se permita generar acciones preventivas tendientes a dificultar las actividades delictivas en el ciberespacio, donde también se favorezcan escenarios de rápida recuperación y protección de los datos.

Cuadro 5
Nivel de madurez al año 2020 de los países analizados y sus avances en legislación relacionada con la ciberseguridad

	Relevamiento 2020					Cambios 2022
	1. Inicial	2. Formativa	3. Consolidada	4. Estratégica	5. Avanzada	
Argentina		X				Sin cambios
Brasil			X			Sin cambios
Chile		X				**Ley 21459**. Deroga la ley Nº 19233 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest
Colombia			X			**Decreto 088-24012022**. Estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea. **Decreto 255-23022022**. Por el cual se adiciona la Sección 7 al Capítulo 25 de la Parte 2 del Libro 2 del Decreto 1074 de 2015. Normas corporativas vinculantes para la certificación de buenas prácticas en protección de datos personales y su transferencia a terceros países. **Decreto Nº 338-08032022**. Establece los lineamientos generales para fortalecer la gobernanza de la seguridad digital y crea el modelo y las instancias de gobernanza de seguridad digital entre otras disposiciones. **Decreto nº 767-16052022**. Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Ecuador		X				**Oficio Nº MINTEL-MINTEL-2022-0975-O – 09082022.** Socialización de la aprobación de la Estrategia Nacional de Ciberseguridad de Ecuador.
México			X			Sin cambios
Panamá		X				Sin cambios
Perú		X				Sin cambios
República Dominicana		X				Sin cambios
Uruguay				X		Sin cambios

Fuente: Elaboración propia.

II. Recomendaciones generales

A. Un escenario de crecientes amenazas requiere un cambio de estrategia

Al profundizar en la problemática y entender que las tecnologías exponenciales traerán en los próximos años nuevos retos que aún no se logran percibir, todo apunta a la necesidad de establecer distintas acciones, tales como la del Foro Económico Mundial que cuenta con una plataforma global, independiente e imparcial destinada a fomentar el diálogo internacional y la colaboración entre la comunidad global de ciberseguridad, tanto en el sector público como en el privado. Lo que se busca entonces en esta iniciativa, es cerrar la brecha entre los expertos en ciberseguridad y los tomadores de decisiones en los niveles institucionales más altos para reforzar la importancia de la ciberseguridad como una prioridad estratégica de importancia mayor. Desde esta comunidad, se identifican tres prioridades clave de trabajo:

- **Creación de resiliencia cibernética**: mejorar la resiliencia cibernética mediante el desarrollo y la ampliación de soluciones con una visión centrada en el futuro, al mismo tiempo que en la promoción de prácticas efectivas en todos los ecosistemas digitales.
- **Fortalecimiento de la cooperación global**: aumentar la cooperación global entre las partes interesadas públicas y privadas que fomenten una respuesta colectiva a la ciberdelincuencia, y a su vez, aborde conjuntamente los principales desafíos de seguridad.
- **Comprender las redes y las tecnologías futuras**: identificar los futuros desafíos y oportunidades de ciberseguridad relacionados con las tecnologías de la Cuarta Revolución Industrial, para encontrar soluciones que ayuden a generar confianza (WEF, 2022).

De igual manera, es importante notar la necesidad de trabajar en los sistemas de educación de base al alcance de toda la sociedad, de manera que en las próximas décadas la ciberseguridad sea de dominio y conocimiento general. En la iniciativa del Foro Económico Mundial (WEF, por sus siglas en inglés), antes mencionada, revelan que la demanda de especialistas en ciberseguridad ha crecido 350% desde el año 2013 y que en 2025 el déficit de profesionales en la especialidad alcanzaría los 3.5 millones

de personas (WEF, 2022). Dentro de los módulos de capacitación ofrecidos por el WEF, se menciona que los más demandados incluyen resiliencia cibernética, higiene cibernética y seguridad de aplicaciones, lo cual refleja cómo las personas están priorizando cómo prevenir y prepararse para un ataque cibernético y cómo crear aplicaciones que puedan ayudarlos a hacer negocios de manera segura.

Las empresas globales más importantes proveedoras de servicios y equipamiento de ciberseguridad, opinan de manera muy similar, afirmando que el crecimiento sostenido de los ataques en América Latina presenta cifras interanuales de 24% entre 2020 y 2021 (Diazgranados, 2021). Esto plasma de manera evidente que se requiere cambiar la estrategia de defensa de detección para poder transformarla en prevención, dejando atrás el modelo de defensa tipo fortaleza o por capas, como se diseñan los sistemas de protección física y como se describe en la norma 27002 (ISO/IEC, 2005), para avanzar hacia un modelo de blindaje unitario y de autorizaciones instantáneas. Esto obedece a la ubicuidad con el que actualmente cuentan, tanto el origen de la amenaza como el activo a proteger, lo cual profundiza el modelo de ciberinmunidad que la CEPAL viene desarrollando desde sus informes publicados en 2020 (CEPAL, 2020), modelo que no se construye con la implementación de uno o un conjunto de equipamientos tecnológicos, sino que requiere un plan de trabajo que permita transitar desde la realidad actual hacia la situación necesaria del futuro.

Una posible estrategia recomendable, sería comenzar este camino con una evaluación basada en modelos internacionales, otorgándole un enfoque práctico. Una recomendación es el marco para Mejorar la Ciberseguridad de las Infraestructuras Críticas del *National Institute for Standards and Technology (NIST)* de Estados Unidos de América, en donde se establece una tendencia de adopción, siendo considerada eficaz en un contexto de innovación tecnológica, ya que se mantiene neutral a la tecnología propiamente dicha, apoyándose en estándares, directrices y prácticas internacionales, administradas y actualizadas por la propia industria tecnológica. Las herramientas y métodos disponibles dentro del modelo para lograr los resultados reconocen la naturaleza global de los riesgos de ciberseguridad y evolucionan con los avances tecnológicos y los requisitos comerciales provenientes del mercado.

A partir de esas normas, directrices y prácticas, el marco NIST proporciona una taxonomía y mecanismo comunes para que las organizaciones puedan:

- Describir su postura actual hacia la ciberseguridad,
- Explicitar objetivamente su estado en ciberseguridad,
- Identificar y priorizar las oportunidades de mejora en el contexto de un proceso continuo y repetible,
- Evaluar el progreso hacia el estado esperado,
- Comunicar entre las partes interesadas internas y externas sobre el riesgo de ciberseguridad.

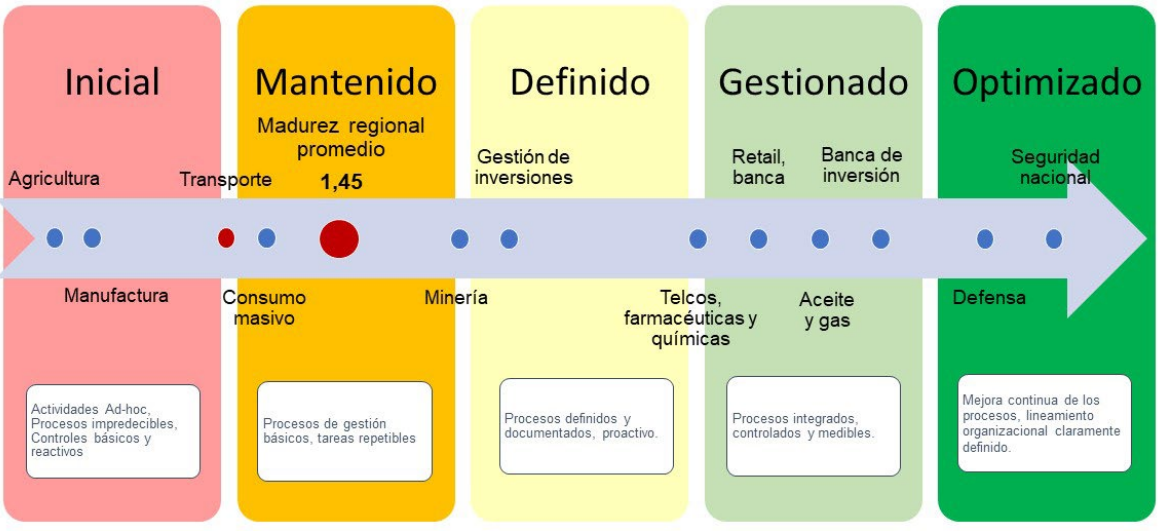
Este enfoque unificado y práctico para gestionar el riesgo de ciberseguridad para las infraestructuras críticas y las organizaciones en general, reconoce que las mismas seguirán teniendo riesgos inherentes a cada actividad, como amenazas, vulnerabilidades y diferentes tolerancias de riesgo, como la forma de personalizar la gestión de la seguridad. No obstante, la aplicación del marco NIST (véase el diagrama 2) se orienta por las organizaciones que puedan determinar las actividades que son importantes para la prestación de servicios críticos, facilitando de esta manera, la priorización de las inversiones para maximizar el beneficio logrado en la estrategia de ciberseguridad (NIST, 2022). Esto sería, particularmente beneficioso para las PYMES, que llegan a generar el 60% del empleo productivo en Latinoamérica y el Caribe (CAF, 2019), representando hasta el 13% del mercado de ciberseguridad. Las PYMEs invierten en promedio menos de U$D500 en ciberseguridad, y lo hacen en soluciones que se colocan en la producción, por lo general *out-of-the-box*, es decir, con configuraciones de fábrica, lo que en consecuencia implica que en la mayoría de los casos no sean una barrera difícil de atravesar, convirtiéndose en objetivos lucrativos para los ciberdelincuentes. (Pawar, 2022).

Según información suministrada por la consultoría internacional KPMG basada en las consultorías realizadas a nivel global se conforma el diagrama 2, con una escala de la medición promedio de madurez en la gestión de la ciberseguridad por rubro, donde se puede observar con preocupación el lugar que ocupan en ella en sector transporte, pieza fundamental de la logística y el comercio internacional, y el promedio de madurez regional, lo cual ilustra el largo camino que queda por recorrer en ambos casos.

Diagrama 2
Mejorar la Ciberseguridad de las Infraestructuras Críticas del National Institute for Standards and Technology

Fuente: Elaboración propia basado en información del Institute for Standards and Technology (NIST).

Diagrama 3
Nivel global de madurez de la gestión en ciberseguridad de las diferentes instituciones según criterio NIST



Fuente: Elaboración propia basada en información suministrada por KPMG.

Particularmente en la categoría "Prevenir" es importante cambiar el paradigma de las últimas décadas de *prepararse para **evitar** el ataque*, propio del modelo comentado previamente de defensa física al estilo fortaleza, por un enfoque más granular y dinámico basado en estar dispuestos para ***recibir*** el ataque, dando por hecho que, tarde o temprano, éste ocurrirá. Para este enfoque, podría ser apropiado tomar en cuenta el modelo desarrollado por Forrester denominado *Zero Trust* (Rose, Borchert, Mitchell, & Connelly, 2020).

El modelo de seguridad *Zero Trust* fue desarrollado en 2010 y se trata de un conjunto de pautas de diseño de sistemas y una estrategia coordinada, basada en el paradigma de que las amenazas existen tanto dentro como fuera de los límites tradicionales de la red. Este modelo utiliza el principio rector de *"nunca confíes, siempre verifica"*. No existe ninguna predisposición sobre el nivel de confiabilidad hacia los usuarios, los equipos participantes de la comunicación o conjuntos de datos involucrados[13].

El modelo de seguridad Zero Trust inicialmente niega todo tipo de acceso a la información y datos desde las aplicaciones. Se logra la prevención de amenazas otorgando solo acceso a redes y cargas de trabajo utilizando políticas monitoreadas mediante una verificación continua, contextual y basada en el riesgo entre los usuarios y sus dispositivos asociados. *Zero Trust* plantea y defiende los siguientes tres principios básicos:

i) Todas las entidades no son de confianza por defecto,

ii) Se aplica el acceso con privilegios mínimos,

iii) Se implementa un monitoreo integral de la seguridad.

Las técnicas para implementar según estos tres principios son:

- Denegar de manera predeterminada.
- Dar acceso solo por política.
- Utiliza los items anteriores para datos, cargas de trabajo, usuarios, dispositivos.
- Dar acceso con privilegios mínimos y explícitos.
- Monitorear permanentemente la seguridad.
- Verificar los escenarios basándose en el riesgo (Holmes & Burn, 2022).

Una situación particular que se ha destacado a lo largo del estudio, y que a la vez es uno de los pilares del modelo de *Zero Trust*, es la necesidad de encontrar mecanismos que sean capaces de elevar el nivel de confianza al momento de realizar la autenticación. Un caso para observar, son las dificultades que presenta la delegación en las personas, la creación de contraseñas difíciles de adivinar y fáciles de recordar, que además no sean repetidas para cada sitio o aplicación y, como si con esto el panorama no fuera complejo, también se pueda recordar cual se usa en cada lugar sin tener un registro escrito fácilmente vulnerable. Es preciso pues recordar, que la autenticación debería hacerse con tres factores, o al menos dos de los tres que se mencionan a continuación:

- 1er factor: algo que la persona (y solo la persona) **conoce**,
- 2do factor: algo que la persona **posee**,
- 3er factor: algo que la persona **es** (Pearson, 2011).

Ha sucedido a lo largo del tiempo, en los años en los que los sistemas eran más cerrados y para poder accederlos se requería de un primer acceso físico al lugar, por lo que esta inaccesibilidad suponía el

[13] Zero Trust fue creado por John Kindervag, quien desarrolló la estrategia mientras trabajaba en Forrester Research.

factor de algo que la persona poseía para lograr el acceso, entonces, con el paso de los años se fue confiando cada vez más, solo en el primer factor. No obstante, esta situación no solo se transformó en un problema, porque había sido trasladado a la buena voluntad de las personas la construcción de contraseñas robustas, sino que además el poder de cómputo fue creciendo con el tiempo y las técnicas para deducir contraseñas se fueron mejorando, al punto de poder descubrir una contraseña formada por 8 caracteres con la mayor complejidad de combinaciones posibles en tan solo ocho horas (BusinessTech, 2022). Por tanto, es necesario volver a contar con un segundo factor en posesión de la persona que se va a identificar. Este segundo factor actualmente se realiza con envíos de códigos por SMS o aplicaciones móviles que generan un código a modo de *token,* los cuales deberían ser utilizados en tantas plataformas como sea posible, ya que el tiempo que transcurre entre un código generado y el siguiente, en general es mucho menor al tiempo que lleva descubrir la contraseña. Por este motivo, un atacante que pretenda obtener acceso descifrando una contraseña, cuando intente utilizarla, la misma ya habrá cambiado como consecuencia del cambio automático del segundo factor. Para sistemas críticos que ameriten seguridad extrema, es recomendable sumar métodos biométricos para representar el tercer factor.

En la actualidad, la combinación de los tres factores se está transformando en algo asequible, por ejemplo, utilizando el teléfono móvil. El mismo se transforma en algo que la persona **tiene**, desbloquearlo a través de una contraseña es algo que la persona **conoce** y sumar la huella es algo que la persona **es**, por lo tanto acceder a una aplicación móvil utilizando estos tres parámetros, representa el uso de los tres factores de autenticación, por lo cual algunas soluciones actuales, están basando la autenticación presentando el teléfono desbloqueado para ser utilizado como método de autenticación (Authena, 2022).

Los sistemas convencionales y de uso más común pueden resultar complejos para realizar estas adecuaciones, por lo que es conveniente diseñar esta transición que se impone de manera natural como el punto más importante en la reducción de riesgos.

Diagrama 4
¿Cuánto tiempo lleva descubrir una contraseña?

Número de caracteres	Solo números	Letras minúsculas	Letras mayúsculas y minúsculas	Números, mayúsculas y minúsculas	Números, letras mayúsculas y minúsculas y símbolo
4	Instantáneamente	Instantáneamente	Instantáneamente	Instantáneamente	Instantáneamente
5	Instantáneamente	Instantáneamente	Instantáneamente	Instantáneamente	Instantáneamente
6	Instantáneamente	Instantáneamente	Instantáneamente	1 segundo	5 segundos
7	Instantáneamente	Instantáneamente	25 segundos	1 minuto	6 minutos
8	Instantáneamente	5 segundos	22 minutos	1 hora	8 horas
9	Instantáneamente	2 minutos	19 horas	3 días	3 semanas
10	Instantáneamente	58 minutos	1 mes	7 meses	5 años
11	2 segundos	1 día	5 años	41 años	400 años
12	25 segundos	3 semanas	300 años	2 mil años	34 mil años
13	4 minutos	1 año	16 mil años	100 mil años	2 millones de años
14	41 minutos	51 años	800 mil años	9 millones de años	200 millones de años
15	6 horas	Mil años	43 millones de años	600 millones de años	15 billones de años
16	2 días	34 mil años	2 billones de años	37 billones de años	1 trillón de años
17	4 semanas	800 mil años	100 billones de años	2 trillones de años	93 trillones de años
18	9 meses	23 millones de años	6 trillones de años	100 trillones de años	7 CM años

Fuente: Hive Systems.

Las acciones ya conocidas y consideradas como práctica estándar como mantener actualizados software y hardware, o como la de tener una adecuada agenda de respaldos con verificaciones periódicas de recuperación, siguen siendo acciones mínimas necesarias que no van a perder vigencia ni van a ser reemplazadas durante los próximos años. Sin embargo, y de acuerdo con los últimos eventos donde los atacantes han logrado tener acceso a los sistemas de respaldo, se debería poner especial atención en mantener la inmutabilidad de los medios físicos donde se guardan las copias con medidas simples, como realizarlas en un medio extraíble, que podría ser un disco extraíble USB para volúmenes bajos, o cintas magnéticas para mayores volúmenes, pero siempre retirándolo físicamente una vez ya grabada la información.

Otras afectaciones ocurridas en los ataques tienen su origen en las estaciones de trabajo distribuidas en la red lo cual desencadena en algunas recomendaciones en relación con ellas o en la propia red. En el primer caso, los antivirus y mantener las actualizaciones al día, siguen siendo necesarios como un estándar básico, pero una medida adicional recomendable es pensar en soluciones que protejan el equipo de acciones desconocidas, como podría ser la aparición de un *malware* que explote una *vulnerabilidad de día cero*[14], para lo cual se pueden utilizar productos de tipo *Endpoint Detection and Response (EDR)*[15] cuya función principal es detectar actividades anómalas en los equipos asignados a los usuarios y tomar acción inmediata de aislamiento en caso de encontrarse actividades no permitidas.

Considerando la actividad de la red de datos, y entendiendo que su misión principal es comunicar, mientras que a lo largo del tiempo se han anexado y mejorado funciones de seguridad, es necesario mencionar que los protocolos de comunicación más comunes no lo hacen de forma segura de manera predeterminada. Esto significa que con poco esfuerzo se podría obtener información confidencial o los propios datos de autenticación, si las medidas de seguridad no son las correctas. Una buena manera de mitigar este importante riesgo es mediante la encriptación de los paquetes de datos que circulan en la red para que solo puedan ser leídos por los equipos destinatarios, práctica que se conoce como encriptación de extremo a extremo o con su definición nativa como *end-to-end encryption.* De esta manera, cualquier equipo que logre interceptar los paquetes que conformen una comunicación con la intención de obtener información de valor o directamente las contraseñas ingresadas en algún momento por los usuarios, no obtendrá más que información cifrada que no resultará legible (CISA, 2022).

Se podría concluir respecto a la estrategia a adoptar para dar tratamiento apropiado a los riesgos relacionados con la ciberseguridad, que el camino señalado en el informe preparado por la CEPAL en el año 2021, anticipaba un enfoque apropiado de inmunidad cibernética muy dinámico, con un espíritu de aprendizaje permanente en el que el sistema se va alimentado y fortaleciendo a través de su evolución, mientras que reacciona de manera favorable a las nuevas amenazas, lo cual en la actualidad suma herramientas de gestión, como el Marco para Mejorar la Ciberseguridad de las Infraestructuras Críticas del NIST y el modelo *Zero Trust*, y técnicas como las prácticas de múltiples factores para realizar la autenticación, EDR y encriptación de extremo a extremo, entre otras desarrolladas a lo largo del documento.

B. ¿Cuáles son las principales tendencias hacia el futuro?

La inteligencia artificial es una de las tecnologías clave de la 4ta revolución industrial que, tal como lo menciona Klaus Schwab, está haciendo difusos los límites entre el mundo físico, digital y biológico (Schwab, 2016). Dentro de este cambio, los ciberataques y su contrapartida, la ciberdefensa, están

[14] Una vulnerabilidad de día cero o Zero Day, es un tipo de vulnerabilidad recientemente descubierta y que aún no tiene un parche que la solucione. Fuente: https://www.osi.es/es/actualidad/blog/2020/08/28/que-es-una-vulnerabilidad-zero-day.

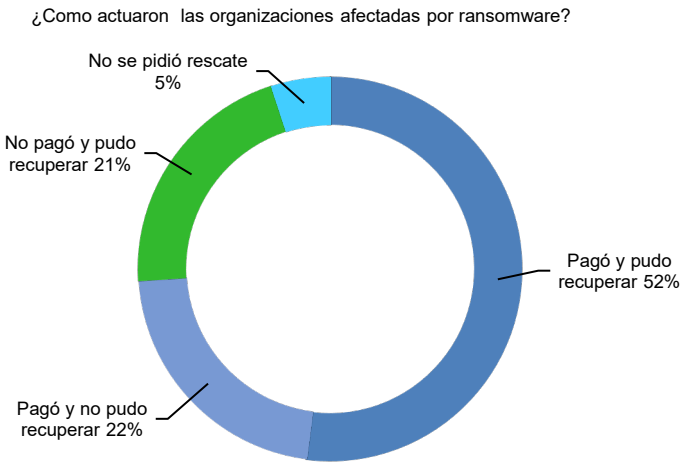
[15] Endpoint Detection and Response (EDR) es un enfoque integrado en capas para la protección de endpoints que combina el monitoreo constante en tiempo real y el análisis de datos de endpoints con una respuesta automatizada basada en reglas. Fuente: https://www.checkpoint.com/es/cyber-hub/what-is-endpoint-detection-and-response/.

afectados por las mismas herramientas tecnológicas que el resto de las actividades, lo cual podría hacer creer que pronto se dé un enfrentamiento entre máquinas y algoritmos, tanto de ataque como de defensa.

Sin embargo, se debe recordar que hay problemas que los humanos resuelven de manera muy sencilla, mientras que a la máquina le llevaría mucho esfuerzo resolver, por ejemplo, aquellas relacionadas con la intuición y la creatividad (Daugherty, 2018). Si bien actualmente se requieren 45 minutos en promedio descubrir un ataque de ransomware, con herramientas automatizadas esto podría hacerse en segundos o incluso en menos tiempo (Murphy, 2022). Sin embargo, el estado de avance de este momento deja entrever que, si bien las etapas iniciales de un ataque y la defensa pueden realizarse con tareas automáticas y de inteligencia artificial, aún existe un terreno en el cual la intervención humana del lado de la defensa sigue siendo una tarea clave, más precisa y eficiente si es ejecutada por personas, por ejemplo, la verificación de los falsos positivos y el entrenamiento permanente del sistema cuando aparecen nuevos patrones de uso. De hecho, los sistemas entrenados son capaces de reconocer y actuar con situaciones para las que fueron diseñados. Por lo tanto, hay un largo camino por delante para que las máquinas puedan, por si solas, actuar en situaciones desconocidas y, actualmente se recomienda avanzar en este campo con una configuración híbrida de analistas de seguridad y la aplicación de inteligencia artificial en una capa inferior.

A principio del año 2022, la firma Veeam dedicada a soluciones de respaldo y replicación de datos, publicó un informe en el que asegura que solo 52% de las organizaciones afectadas por ransomware en 2021 recibieron sus datos después de haber pagado un rescate por ellos, mientras que el 22% pagó sin poder recuperar la información y solo, un 21% decidió no pagar y recuperó la información y las operaciones. El 5% restante, nunca recibió pedido de rescate, como es posible observar en el gráfico 9 (Veeam , 2022).

Gráfico 9
Recuperación de la información en un ataque de ransomware



Fuente: Veeam.

Cabe reflexionar que el hecho de pagar no es una opción en la cual las organizaciones puedan descansar. Básicamente por dos razones, porque el pasado indica que pagar no asegura la recuperación, ya que se deposita la confianza en un grupo que no se puede rastrear ni reclamar si es que no hay respuesta del pago, y porque pagar significa seguir alimentando el lucro de la actividad y por lo tanto el volumen y la frecuencia de los ataques. Sin embargo, a pesar de las recomendaciones de tomar un plan de acción preventivo, hay casos en los cuales las organizaciones se encuentran sin opciones y las

decisiones tienden a tomarse caso a caso sopesando el precio de la demanda de rescate contra el costo potencial de no pagar, que podría incluir pérdida de datos, interrupción del negocio o riesgo legal si los clientes deciden demandar en el caso de que los atacantes filtraran sus datos. Un ejemplo es el sector legal y los datos confidenciales de clientes, a menudo optan por pagar para evitar el posible impacto a la reputación de la empresa (Murphy, 2022).

Es de suponer que, en el futuro cercano, el lucro que obtienen los grupos atacantes a través del ransomware provenga del valor de los datos secuestrados y ya no por la continuidad operativa de la red, valor que estará dado por la confidencialidad de estos, ya sea por la sensibilidad o por el cumplimento regulatorio. Por este motivo las pólizas de seguro que actualmente se pueden contratar y cubren, entre otros, los riesgos de ciberseguridad, solicitan contar con un relevamiento del nivel de madurez de la ciberseguridad del asegurado realizado sobre la guía de estándares internacionales como la ISO 27000 o el modelo de seguridad del NIST, adaptando la economía de este mercado tan importante a las nuevas dimensiones de las variables que la seguridad cibernética representa en la matriz corporativa de riesgos.

III. Conclusiones y recomendaciones

A lo largo de la investigación realizada, durante el período 2020-2022, se observa un importante crecimiento en la cantidad de incidentes ocurridos que han afectado las cadenas logísticas y la infraestructura física de la región. A través de un relevamiento de incidentes en la región vía distintos medios, informes globales y de estadísticas de los centros de atención de incidentes de ciberseguridad, etc. ha sido posible recoger evidencia sobre la severidad de los ataques y sus principales impactos.

El trabajo de concientización realizado en los últimos años, producto de la acelerada digitalización, la pandemia del COVID, el efecto sobre las cadenas de suministro, (entre otras cosas) ha instalado la idea de que la ciberseguridad representa un riesgo mayor que debe ser atendido, a todos los niveles de la organización. El proceso de seguimiento y control se puede ver afectado de igual forma y afectar así la confianza de inversionistas, clientes y grupos interesados.

Las respuestas a los incidentes ocurridos en grandes instituciones privadas relacionadas con la continuidad operativa muestran avances significativos respecto al informe anterior (CEPAL, 2021), aunque los mismos indicadores no parecen reflejarlo en las organizaciones de menor tamaño, ni en las instituciones gubernamentales de los países, situación que se extiende a todo tipo de institución (pública y privada) cuando se focaliza en confidencialidad de los datos.

En los últimos años, las mejoras en ciberseguridad de los gobiernos se han manifestado en estrategias y políticas declaradas. Sin embargo, en la práctica, salvo el caso de Colombia, no se encontraron evidencias sobre avances significativos que beneficien a las instituciones públicas o ayuden a las pymes preventivamente o en su recuperación, cuando estas son afectadas por un incidente, sobre todo cuando estos ponen en peligro su economía. De no mostrar mejoría, las brechas digitales pueden ampliarse con consecuencias para la recuperación de las economías de la región. Es urgente abordar esta situación, debido a que las tecnologías exponenciales, por su capacidad de hacer crecer exponencialmente la eficiencia de quienes las implementan, han comenzado a trepar en el segmento de la curva donde empieza el crecimiento vertical, y el eje horizontal representa el tiempo. De prolongarse el tiempo de la transformación digital, la

región estará expuesta a una brecha digital que crecerá exponencialmente. Para contrarrestar los impactos, se recomienda tomar las siguientes acciones:

- Implementar marcos normativos / regulatorios basados en estándares internacionales que ayuden a fortalecer la ciberseguridad de las instituciones. Una posible alternativa, podría ser el modelo de gobernanza planteado por el NIST.
- Difundir la importancia que la ciberseguridad representa para los estados y las acciones de instituciones públicas que los ciudadanos tienen a su alcance para protegerse de ataques.
- Revisar los planes de educación, de manera de incluir el conocimiento y prevención de los riesgos cibernéticos desde las etapas tempranas de enseñanza de la sociedad. La incorporación de la protección de datos personales en la currícula de contenidos ayudaría a mejorar los niveles de madurez en la protección de los derechos de los ciudadanos, y la comprensión que cada individuo tiene sobre el valor que los datos tienen en la 4ª. revolución industrial.
- La etapa de creación de los CSIRT como instituciones públicas al servicio de todos los ciudadanos y las organizaciones pareciera haberse cumplido satisfactoriamente en la región. Sin embargo, se debería revisar la capacidad de respuesta de estos equipos para que efectivamente puedan ser el soporte adecuado y oportuno ante la aparición de incidentes de seguridad, articulando acciones con las fuerzas de orden público nacional, regional e internacional en caso necesario.
- Individualmente los consejos directivos de las organizaciones deberían analizar el grado de madurez en seguridad cibernética y fijar, a partir de los resultados, un proceso de mejora continua, que minimice el riesgo y funcione como herramienta para generar confianza en la integridad de la cadena de distribución.
- Continúan siendo las personas la principal causa-raíz por la que ingresa el primer vector de ataque en los incidentes de seguridad, por lo tanto, la concientización del personal en seguridad es importante. Se deben considerar los distintos tipos de programas de concientización adaptables al tamaño, economía y naturaleza de cada organización que hoy ofrece el mercado.
- A nivel técnico, continuar con la revisión permanente de las medidas de protección de perímetro tecnológico tradicionales, adecuados respaldos de información para obtener inmutabilidad de los repositorios de estos. De igual manera mantener actualizados los equipos de usuario final y evaluar la posibilidad de incluir en ellos tecnologías de tipo EDR.
- Para proteger los datos durante la comunicación entre los equipos intervinientes, es conveniente utilizar encriptación de extremo a extremo en las aplicaciones y servicios.
- En la industria de transporte marítimo, especialmente en el rubro de cruceros, revisar que los protocolos utilizados en los procedimientos que utilicen soporte informático o transmisión de datos cuenten con medidas de autenticación y autorización adecuados. Poner especial atención en aquellas comunicaciones de datos que están basadas en sistemas de VHF.
- Implementar una estrategia de confidencialidad de los datos basada en el modelo *Zero Trust*, focalizado en un modelo de autenticación de dos o más factores, recomendación especialmente importante para aquellas organizaciones que deban cumplir con el GDPR o quienes administren datos sensibles de terceros, como por ejemplo los de salud.
- Poner a prueba permanente los planes de recuperación ante desastre como un ejercicio de preparación para entrar en acción.
- En caso de ser víctima de ransomware, la acción preventiva debe ser la primera opción y no el pago de rescates. Si la única opción fuese recurrir al pago, se recomienda asesoramiento externo y conducir el proceso con personal especializado en recuperación de ransomware.

Bibliografía

Holmes, D., & Burn, J. (2022), *Forrester*. Obtenido de The Definition Of Modern Zero Trust: https://www.forrester.com/blogs/the-definition-of-modern-zero-trust/.

Amerise, A. (2022), *BBC News.* Obtenido de "Estamos en guerra": 5 claves para entender el ciberataque que tiene a Costa Rica en estado de emergencia: https://www.bbc.com/mundo/noticias-america-latina-61516874.

Authena (27 de 07 de 2022). Obtenido de Authenticate via NFC Technology To Prevent Product Tampering: https://authena.io/authenticate-via-nfc-technology-to-prevent-product-tampering/.

BID y OEA (2020). *Observatorio CIberseguridad.* Obtenido de Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe: https://observatoriociberseguridad.org/#/home.

BusinessTech. (02 de 04 de 2022). Obtenido de How long it takes hackers to crack your password based on how many characters it has: https://businesstech.co.za/news/it-services/572976/how-long-it-takes-hackers-to-crack-your-password-based-on-how-many-characters-it-has/.

CAF. (25 de 04 de 2019). *Índice de Políticas PYME: América Latina y el Caribe 2019* . Obtenido de https://www.caf.com/es/actualidad/noticias/2019/04/indice-de-politicas-pyme-america-latina-y-el-caribe-2019/.

Carlson, B. (07 de 10 de 2021). *CSO*. Obtenido de Top cybersecurity statistics, trends, and facts: https://www.csoonline.com/article/3634869/top-cybersecurity-statistics-trends-and-facts.html.

Comisión Económica para América Latina y el Caribe (CEPAL) (2023), "Perspectivas del Comercio Internacional de América Latina y el Caribe, 2022" (LC/PUB.2022/23-P), Santiago.

_____ (2021). *CEPAL.* Obtenido de Estado de la ciberseguridad en la logística de América Latina y el Caribe: https://www.cepal.org/es/publicaciones/47240-estado-la-ciberseguridad-la-logistica-america-latina-caribe.

_____ (2020). *Boletin FAL 382.* Obtenido de La ciberseguridad en tiempos del COVID-19 y el tránsito hacia una ciberinmunidad: https://www.cepal.org/es/publicaciones/46275-la-ciberseguridad-tiempos - covid-19-transito-ciberinmunidad.

Checkpoint. (10 de 2022). *Check Point Research.* Obtenido de Third quarter of 2022 reveals increase in cyberattacks and unexpected developments in global trends: https://blog.checkpoint.com/2022/10/26/third-quarter-of-2022-reveals-increase-in-cyberattacks/.

CISA. (10 de 02 de 2022). *Alert (AA22-040A)*. Obtenido de 2021 Trends Show Increased Globalized Threat of Ransomware: https://www.cisa.gov/uscert/ncas/alerts/aa22-040a.

Cruceros, P. (15 de 06 de 2022). *https://portalcruceros.cl/global-data-gastos-por-ciberseguridad-en-turismo-superaran-usd-2-mil-millones-en-2025/*.

Daugherty, P. R. (2018). Human + machine: Reimagining WorkHarvard Business Review Press . *Harvard Business Review Press*.

Díaz, R. M. (2022). *"Ciberseguridad en cadenas de suministros inteligentes en América Latina y el Caribe".* Santiago: Comisión Económica para América Latina y el Caribe (CEPAL). Obtenido de Documentos de Proyectos (LC/TS.2022/70).

Diazgranados, H. (2021), *Kaspersky Daily*. Obtenido de Ciberataques en América Latina crecen un 24% durante los primeros ocho meses de 2021: https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/.

Drone, N. (2021), *https://alsum.co/ataques-ciberneticos-a-la-industria-maritima-en-los-ultimos-10-anos/*.

EEUU, G. C. (04 de 07 de 2022). *https://www.infobae.com/america/wapo/2022/07/04/ciberpiratas-la-nueva-amenaza-de-los-mares/*.

Gartner. (2021), *The Top 8 Cybersecurity Predictions for 2021-2022.* Obtenido de A focus on privacy laws, ransomware attacks, cyber-physical systems and board-level scrutiny are driving the priorities of security and risk leaders. https://www.gartner.com/en/articles/the-top-8-cybersecurity-predic tions-for-2021-2022.

Ginter, A., y Hale, G. (2021), *OT Security Incidents. .* Obtenido de 2021 Trends and Analyses: https://waterfall-security.com/wp-content/uploads/2022/05/OT-Security-Incidents-ebook_FINAL.pdf?utm_campaign=2021%20OT%20Incidents&utm_medium=email&_hsmi=222712301&_hsenc=p2ANqtz-8LiaRmpYuWN_UMzEI91PN5Lg9NdbHyRhDyaeEO5StuZ8cVCtPtbdYIoUo_RnC8jk9LzdebBmLOyK.

Global Cybersecurity Outlook 2022, World Economic Forum, Insight Report, January https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf.

Godin, S. (2014), *Justifica tu respuesta.* Obtenido de 10 Frases de Seth Godin que todo docente debería aplicar a su profesión: https://justificaturespuesta.com/10-frases-de-seth-godin-que-todo-docente-deberia-aplicar-su-profesion/.

Gutiérrez, T. (2022), *LaRepublica.net.* Obtenido de $38 millones en pérdidas al día generan hackers al sector exportador: https://www.larepublica.net/noticia/38-millones-en-perdidas-al-dia-generan-hackers-al-sector-exportador.

HIPAA Journal (2021), *HIPAA Journal.* Obtenido de Ransom Disclosure Act Requires Disclosure of Payments to Ransomware Gangs Within 48 Hours: https://www.hipaajournal.com/ransom-disclosure-act-requires-disclosure-of-payments-to-ransomware-gangs-within-48-hours/.

_____(2021), *HIPAA Journal.* Obtenido de Lawsuit Alleges Ransomware Attack Resulted in Hospital Baby Death: https://www.hipaajournal.com/lawsuit-alleges-ransomware-attack-resulted-in-hospital-baby-death/.

Informática Jurídica (2022), *Informática Jurídica*. Obtenido de Legislación Informática: https://www.informatica-juridica.com/legislacion/.

ISO/IEC (2022), obtenido de ISO/IEC 27001 and related standards: https://www.iso.org/isoiec-27001-information-security.html.

_____(2005), *ISO 27000.* Obtenido de Seguridad Física y Ambiental: https://www.iso27000.es/iso27002 _11.html.

KPMG. (2022), *Una triple amenaza en las américas.* Obtenido de https://home.kpmg/ar/es/home/insights/2022/01/kpmg-fraud-outlook-survey-spanish.html.

Learning Security Hub. (2022), *World Economic Forum*. Obtenido de Delivering free and globally accessible cybersecurity training: https://www.weforum.org/impact/cybersecurity-training/.

Mee, P., & Brandenburg, R. (2020), *World Economic Forum.* Obtenido de After reading, writing and arithmetic, the 4th 'r' of literacy is cyber-risk: https://www.weforum.org/agenda/2020/12/cyber-risk-cyber-security-education.

Mishra, S. (2022), *Harvard Law School Forum on Corporate Governance.* Obtenido de ESG and C: Does Cybersecurity Deserve Its Own Pillar in ESG Frameworks?: https://corpgov.law.harvard.edu/2022/11/14/esg-and-c-does-cybersecurity-deserve-its-own-pillar-in-esg-frameworks/.

Murphy, H. (2022), *Financial Times.* Obtenido de Special Report. Navigating Cyber Risk: https://www.ft.com/content/a978b8a6-ebc5-4929-ac63-6be7acb7d738.

NIST. (2022), *Information Technology Laboratory*. Obtenido de Computer Security Resource Center: https://csrc.nist.gov/.

Pastor, J. (2020), *Xataka.* Obtenido de Un ataque ransomware a un hospital en Alemania pudo ser el causante de la muerte de una paciente: https://www.xataka.com/seguridad/ataque-ransom ware-a-hospital-alemania-pudo-ser-causante-muerte-paciente.

Pawar, P. (2022), Obtenido de 50+ Alarming Cybersecurity Statistics 2022 Facts and Trends That Users Need To Know : https://www.enterpriseappstoday.com/stats/cybersecurity-statistics.html.

Pearson. (2011), *Pearson IT Certification SSCP*. Obtenido de Understanding the Three Factors of Authentication: https://www.pearsonitcertification.com/articles/article.aspx?p=1718488.

Rockwell Automation Inc. (2022), *Rockwel Automation.* Obtenido de 2022 Critical Infrastructure Research Report: https://www.rockwellautomation.com/en-us/capabilities/industrial-cybersecurity/services/criticalinfrastructurepreparednessreport.html?utm_medium=google&utm_source=CPC.&utm_campaign=MultiInitiative_MultiAudience_Global_XX_XX_CMP-04271-Z1J6R1&utm_content=.

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020), *NIST Special Publication 800-207.* Obtenido de Zero Trust Architecture: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

Schwab, K. (2016), *The Fourth Industrial Revolution: what it means, how to respond.* Obtenido de World Economic Forum: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/.

UNCTAD (2018). Review of Maritime Transport 2018. UNCTAD/RMT/2018.

Unión Internacional de Telecomunicaciones (UIT), 2022. "Global Cybersecurity index 2020". https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.

Varonis. (2021), *Varonis Systems Inc.* Obtenido de 2021 Data risk report: https://info.varonis.com/hubfs/docs/research_reports/2021-Financial-Data-Risk-Report.pdf?utm_content=146358482&utm_medium=social&utm_source=twitter&hss_channel=tw-21672993&hsLang=en.

Veeam. (2022), Obtenido de 2022 Ransomware Trends Report: https://go.veeam.com/wp-ransomware-trends-report-2022.

WEF. (2022), *World Economic Forum*. Obtenido de Centre for Cybersecurity: https://www.weforum.org/platforms/the-centre-for-cybersecurity.

World Bank (2022), Financial inclusion is a key enabler to reducing poverty and boosting prosperity. https://www.worldbank.org/en/topic/financialinclusion/overview#1.

Anexos

Anexo 1
Relevamiento de incidentes ocurridos en los países observados entre 2020 y 2022

Tipo de actividad	Argentina	Brasil	Chile	Colombia	Ecuador	México	Panamá	Perú	Rep. Dominicana	Uruguay	Organización afectada	Descripción de la actividad	Impacto D	Impacto C	Impacto I	Tipo de incidente	Fecha de referencia del incidente	Descripción del incidente	Impacto Cualitativo	Impacto Cuantitativo	Impacto Días impacto	Impacto Costo en dólares	Resolución	Fuente
	X										La Serenísima, como empresa reconocida, fue invocada como medio para realizar la estafa	Producción láctea y productos derivados		X	X	Suplantación de identidad-phishing-ingeniería social	1/4/2021	Mediante un link por WhatsApp y redes sociales donde se suplanta la identidad de la empresa láctea La Serenísima. El mensaje se presenta como "¡Celebración del 90 aniversario de La Serenísima!, prometiendo regalos con motivo de la celebración mencionada, solicitando a la vez datos personales del afectado	No identificado	No identificado			La empresa publicó comunicado en redes sociales advirtiendo sobre el engaño	https://www.perfil.com/noticias/actualidad/nueva-estafa-a-nombre-de-la-serenisima-roban-datos-personales-ofreciendo-regalos-por-el-aniversario-numero-90-de-la-compania.phtml
Industria	X										Fábrica Argentina de Aviones-FADEA	La Fábrica Argentina de Aviones «Brigadier San Martín» S. A. es una empresa dedicada a la producción de aeronaves y la investigación aeroespacial, cuya planta está ubicada en la provincia de Córdoba			X	Malware/ estafa/ phishing/ suplantación de identidad	6/4/2021	Transferencias internacionales que suman casi medio millón de dólares realizadas desde la FADEA a "personas aún no identificadas" que "simularon pertenecer" a *Advent Aircrfat Systems* (proveedor dedicado al diseño, fabricación y certificación de productos y componentes de aviones)	Autores desconocidos se hicieron pasar por ambas partes y concretaron la estafa	No aplica	300	500 000	No aplica	https://www.defensa.com/ciberseguridad/ciberataque-hackers-estafa-argentina-fadea-cerca-medio-millon
Estado	X										Instituto de Obra Social de las Fuerzas Armadas	El Instituto de Obra Social de las Fuerzas Armadas es una obra social que presta servicio a las Fuerzas Armadas, la Gendarmería Nacional Argentina y la Prefectura Naval Argentina		X	X	Robo y publicación de datos internos del organismo	29/9/2021	Robo y publicación de datos internos del organismo correspondiente a 1.200.000 afiliados aproximadamente	Hay nombres completos, estado civil, sexo, dirección postal, números de teléfono, correo electrónico y rango de las personas afectadas	El instituto declara que la base de datos afectadas es obsoleta, por lo que los datos son desactualizados			El organismo no tomo ninguna medida, argumentando que se trata de información desactualizada	https://www.lanacion.com.ar/tecnologia/publican-informacion-privada-de-12-millones-de-militares-y-empleados-de-agencias-de- seguridad-nid29092021/
Estado	X										Registro Nacional de las Personas	Registro de la identidad de los ciudadanos de la República Argentina, conteniendo: las direcciones, teléfonos, fotos y número de trámite de DNI, entre otras cosas. Esta información es consultada por organismos públicos y la sociedad privada		X	X	Robo de datos internos del organismo	24/10/2021	Filtración de datos de una cantidad no confirmada de personas registradas	En redes sociales, se publicó el robo de aproximadamente 60.000 registros personales y a modo de prueba confirmatoria de la filtración realizada, fue difundida información sensible de periodistas, políticos, deportistas y artistas reconocidos, entre muchos otros	Considerando los resultados provisorios del Censo 2022 realizado en Argentina, la cantidad de registros sustraídos representa el 0,12% del total de las bases de datos de RENAPER		17 000	El organismo procedió a restringir, en distintos niveles de alcance, el acceso a las bases de datos	https://www.lanacion.com.ar/tecnologia/el-estado-argentino-detecto-mas-del-doble-de-incidentes-informaticos-durante-2021-nid07032022/

Tipo de actividad	Argentina	Brasil	Chile	Colombia	Ecuador	México	Panamá	Perú	Rep. Dominicana	Uruguay	Organización afectada	Descripción de la actividad	Impacto D	Impacto C	Impacto I	Tipo de incidente	Fecha de referencia del incidente	Descripción del incidente	Impacto Cualitativo	Impacto Cuantitativo	Impacto Días impacto	Impacto Costo en dólares	Resolución	Fuente
Estado	X										Cámara Senado de la Nación	Cuerpo legislativo que representa a las jurisdicciones provinciales de la Nación	X	X		Ransomware	12/1/2022	Secuescitro paral de información pública y de tipo sensible	No informado	No informado	2		Recuperación de la información desde copias de respaldo	https://www.infobae.com/politica/2022/01/14/el-senado-de-la-nacion-confirmo-que-sufrio-un-ciberata que-de-piratas-infor maticos-se-logro-recuperar-la-mayo ria-de-la-informacion-relevante/
Comercio	X										Mercado Libre	Comercio electrónico		X		Robo de datos internos de la empresa	8/3/2022	Acceso no autorizado al repositorio de su código fuente	La empresa reconoció haber sido objeto de acceso no autorizado a información de sus usuarios, sin encontrar evidencia de acceso a otros datos sensibles de la misma	Filtración de datos de 300.000 de usuarios de la empresa (casi 140 millones de usuarios activos únicos)			La empresa declaró haber puesto en marcha los protocolos indicados para la situación	https://www.lanacion.com.ar/tecnologia/mercado-libre-confirma-la-filtracion-de-datos-de-300000-usuarios-nid07032022/
Energía	X										Transportadora de Gas del Sur	Transportadora de gas natural. Red 9231 km. Distribuye en siete provincias, siendo la operadora de la red más extensa de América Latina	X	X		Ransomware	1/4/2022	El incidente se detectó contra su sistema SPAC, plataforma de procesamiento de solicitudes, asignación y programación de los volúmenes de gas se cargan en la red de gasoductos	El ciberataque dejó fuera de servicio la página web de TGS, pero no hubo riesgo para la operación en si misma del sistema de gas	No especificada			La empresa declaró haber detectado el ataque lo que permitió minimizar el impacto del mismo, no obstante, reconoció haber operado la aplicación impactada "a ciegas" con un esquema de comunicación de solicitudes de contingencia	https://econojournal.com.ar/2022/04/tgs-logro-resolver-un-ciberataque-que-afecto-un-sistema-virtual-de-gestion-del-sistema-gasifero/
Industria	X										Grupo Ledesma	Compañía azucarera	X	X		Ransomware-Lockbit	1/4/2022	Encriptado de archivos y solicitando un rescate para devolver la información y no publicar lo sucedido	No informado	No se reveló el monto que solicitaron los delincuentes para devolver el acceso a los archivos se presume que la cifra fue grande			Dada la reserva tomada por la empresa, se supone se procedió a recuperar la información secuestrada desde copias de respaldo	https://www.americaeconomia.com/empresas-ciberataque-de-latinoamerica-crece
Estado	X										Consejo Nacional de Investigaciones Científicas y Técnicas-CONICET	Organismo dedicado a la promoción de la ciencia y la tecnología en Argentina, dependiente del Ministerio de Ciencia, Tecnología e Innovación de la Nación	X	X		Ransomware	22/4/2022	Las oficinas de la Sede Central del CONICET fueron las únicas afectadas durante el ataque virtual. El mismo fue bajo la modalidad 'ransomware', donde los ciberdelincuentes secuestran información sensible para luego pedir rescate por los datos que robaron	No fueron afectados los servicios críticos	No declarado			Preventivamente se aislaron los servidores críticos y se procedió a recuperar la información secuestrada desde copias de respaldo	https://radiomitre.cienradios.com/sociedad/hackearon-el-sitio-web-del-conicet-robaron-informacion-de-la-sede-central-y-pidieron-rescate/

Tipo de actividad	Argentina	Brasil	Chile	Colombia	Ecuador	México	Panamá	Perú	Rep. Dominicana	Uruguay	Organización afectada	Descripción de la actividad	Impacto D	Impacto C	Impacto I	Tipo de incidente	Fecha de referencia del incidente	Descripción del incidente	Impacto Cualitativo	Impacto Cuantitativo	Días impacto	Costo en dólares	Resolución	Fuente
Tecnología	X										Prominente S.A.	Compañía de soluciones tecnológicas, especializada en automatización de procesos de negocios, desarrollo de software, *big data* y servicios *cloud*	X	X		Ransomware	4/5/2022	Afectó el sistema de emisión de boletos electrónicos para viajes urbanos, corta y mediana distancia en la ciudad de Buenos Aires y aledaños	El hackeo contra los servidores de la empresa Prominente, que provee los servicios de alojamiento para Emova (subterráneos) y Metrovías (ferrocarril Urquiza)	No informado	3		Dada la reserva tomada por la empresa, se supone se procedió a recuperar la información secuestrada desde copias de respaldo	https://www.enelsubte.com/noticias/un-ataque-informati co-prominente-dejo-sin-servicios-subte/
Industria	X										Aceitera General Deheza	Complejo agroindustrial dedicado a la producción de proteínas y aceites vegetales, biodiésel y glicerina refinada	X	X		Ransomware	10/8/2022	Fue detectada una intromisión en los sistemas informáticos. Es por este motivo que se activaron protocolos de seguridad, a fin de realizar un análisis exhaustivo de la situación y se efectuaron las denuncias correspondientes	La empresa declara haber continuado sus operaciones en forma manual	No se reveló el monto que solicitaron los delincuentes para devolver el acceso a los archivos se presume que la cifra fue grande. No obstante, la empresa declaró que no accederá al pago de rescate			La empresa procedió a recuperar la información secuestrada desde copias de respaldo	https://www.memo.com.ar/tribunales/hackeo-aceitera-general-deheza/
Estado	X										Poder Judicial de la Provincia de Córdoba	Administración de justicia a nivel provincial	X	X		Ransomware-PlayCrypt	13/8/2022	Cambia la extensión de todos los archivos afectados a "play"	Afectó la totalidad de los trámites judiciales como las constancias, libramientos de oficios y órdenes de pago peritos, abogados, cuota beneficiarios de alimentaria, entre otros)	Alcanzó a unos 8 mil usuarios del sistema interno y a los cerca de 25 mil abogados matriculados en la provincia			Se tomaron medidas de tipo administrativa: postergación de fechas de vencimiento y se pasó toda la gestión a documentación impresa	https://www.clarin.com/tecnologia/caos-justicia-cordoba-ransomware-expedientes-bloqueados-pagos-suspenso_0_7rJdwF0A58.html
Estado		X									Corte Suprema	El Supremo Tribunal Federal es el más alto tribunal del Poder Judicial de Brasil y posee las atribuciones propias de una Corte Suprema y de un Tribunal Constitucional. Su función institucional es servir de guardián de la Constitución Federal, resolviendo casos que implican lesión o amenaza a esta última	X	X		Ransomware-RansomExx	3/11/2020	Se explotó una cuenta de administrador de dominio que le permitió al ciberdelincuente acceder a los servidores, unirse a los grupos de administración del entorno virtual y, finalmente, cifrar buena parte de las máquinas virtuales	Los jueces, pasantes y trabajadores subcontratados fueron informados de que no podían usar los ordenadores si estos se encontraban conectados a la red del tribunal en el momento del ataque	Fueron cifrados más de 1.200 servidores, en su mayoría máquinas virtuales. Además, fueron destruidas las copias de seguridad de esas máquinas virtuales	6		Suspensión temporal del funcionamiento de los sistemas operativos de los servidores, para proteger la integridad de sus datos. Recuperación de la configuración desde copias de respaldo	https://derechodelared.com/justicia-brasil-ciberataque/

Tipo de actividad	Argentina	Brasil	Chile	Colombia	Ecuador	México	Panamá	Perú	Rep. Dominicana	Uruguay	Organización afectada	Descripción de la actividad	Impacto D	Impacto C	Impacto I	Tipo de incidente	Fecha de referencia del incidente	Descripción del incidente	Impacto Cualitativo	Impacto Cuantitativo	Impacto Días impacto	Impacto Costo en dólares	Resolución	Fuente
Energía		X									Eletronuclear	Empresa estatal responsable por la operación de las dos centrales nucleares	X	X		Ransomware	4/2/2021	Las oficinas administrativas de la estatal fueron blanco de un ataque, los sistemas de la red administrativa no están conectados con los sistemas operativos de las centrales nucleares, por lo que el ataque no llegó a afectar ni amenazar las generadoras por lo que no amenazó el abastecimiento de energía eléctrica al Sistema Interconectado Nacional	Debieron suspenderse temporalmente el funcionamiento de algunos de sus sistemas operativos para proteger la integridad de sus datos	No especificado			Suspensión temporal del funcionamiento de algunos de sus sistemas operativos para proteger la integridad de sus datos. Los sistemas fueron reactivados luego de que los técnicos de la empresa "contuvieran y erradicaran los efectos del ataque, aislaran el virus y realizaran una minuciosa verificación de los activos"	https://www.swissinfo.ch/spa/brasil-ciberataque_la-estatal-nuclear-brasile%C3%B1a-sufri%C3%B3-ciberataque-pero-sin-afectargeneradoras/46345580
Estado		X									Tribunal de Justicia de Rio Grande do Sul -TJ-RS	Administración de justicia a nivel estadual	X	X		Ransomware	1/4/2021	Bloqueo total de las aplicaciones y bases de datos y también de algunos servidores	Fue afectada toda la información procesal almacenada en la base de datos, como archivos confidenciales y datos personales de los empleados, de cumplimiento del impuesto sobre rendimientos y compensaciones, así como información sobre las investigaciones en curso	No informado			Los sistemas fueron reactivados luego de que los técnicos de la empresa "contuvieran y erradicaran los efectos del ataque, aislaran el virus y realizaran una minuciosa verificación de los activos	https://canalcienciascriminais.com.br/sistema-do-tj-rs-e-invadido-por-hackers-que-cobram-resgate-em-bitcoin/
Finanzas		X									BR Partners	Entidad bancaria	X	X		Ransomware	16/4/2021	Inhibición de acceso a las bases de datos	La entidad confesó que fue objeto de un ciberataque, pero aseguró que no hubo transacción monetaria con valores de clientes o grupos, ni accesos a contraseñas y datos que incurran en riesgo financiero	No informado			El banco de inversión anunció que se activaron los protocolos de control y seguridad para contener la amenaza, evaluar y minimizar los impactos. Sin embargo, no reveló a qué información accedieron los delincuentes ni cuál fue la magnitud de la pérdida provocada por este ataque	https://www.americaeconomia.com/empresas-ciberataque-de-latinoamerica-crece
Comercio		X									Grupo de Medicina de Diagnóstico Fleury	Servicios de medicina diagnóstica y tecnología aplicada	X	X		Ransomware-Sodinokibi	22/6/2021	Afectación parcial de las aplicaciones, no afectando las bases de datos	El ataque dejó indisponible parte de sus sistemas y perjudicando las operaciones de los laboratorios, el área dedicada a los resultados de los exámenes, entre otros	Bloqueo total de las bases de datos de laboratorio, datos de imágenes y registros de pacientes			Recuperación de las configuraciones y datos desde copias de respaldo	https://www.tecmundo.com.br/seguranca/219831-grupo-fleury-alvo-ataque-cibernetico.htm

Tipo de actividad	Argentina	Brasil	Chile	Colombia	Ecuador	México	Panamá	Perú	Rep. Dominicana	Uruguay	Organización afectada	Descripción de la actividad	Impacto D	Impacto C	Impacto I	Tipo de incidente	Fecha de referencia del incidente	Descripción del incidente	Impacto Cualitativo	Impacto Cuantitativo	Días impacto	Costo en dólares	Resolución	Fuente
Estado		X									Secretaría del Tesoro Nacional	Administración de las reservas monetarias de Brasil	X	X		Ransomware	13/8/2021	El ataque se realizó contra la red interna de la Secretaría del Tesoro Nacional	La acción no perjudicó los sistemas estructurantes del Departamento del Tesoro Nacional, como el Sistema Integrado de Administración Financiera (Siafi)	No informado			Recuperación de la configuración desde copias de respaldo	https://www.cnnbrasil.com.br/business/sistema-do-tesouro-nacional-sofre-ataque-hacker/
Comercio		X									Renner	Lojas Renner es la mayor empresa brasileña de ropa para grandes almacenes, con sede en Porto Alegre-Rio Grande do Sul	X	X		Ransomware	19/8/2021	Dejó sin servicio a su página web, no afectando las bases de datos	El ataque dejó indisponible la página web de la empresa, impactando negativamente en la comercialización de la misma	No informado	4		La empresa se concentró en para mitigar los efectos causados. Ejecutando el plan de protección y recuperación, con todos sus protocolos de control y seguridad y trabajando para restablecer todas las operaciones	https://www.cnnbrasil.com.br/business/site-da-renner-continua-fora-do-ar-apos-ataque-hacker/
Comercio		X									CVC Corp	Viajes y turismo	X	X		Ransomware	1/10/2021	Dejó sin servicio a su página web, no afectando las bases de datos	El ataque dejó indisponible la página web de la empresa, impactando negativamente en la comercialización de la misma	El lucro cesante debido a la imposibilidad de acceder a la página web			No informado	https://www.cisoadvisor.com.br/cvc-corp-comunica-ataque-site-esta-inoperante/
Comercio		X									Porto Seguro S.A.	Tercera compañía de seguros brasileña más importante	X	X		Inestabilidad de las aplicaciones	15/10/2021	Intento de ciberataque que terminó provocando inestabilidad en los sistemas de la compañía. Los canales de atención de la empresa también se vieron parcialmente afectados	Ralentización de las aplicaciones, no se registraron afectaciones en las bases de datos	No aplica	1		Recuperación de la configuración desde copias de respaldo	https://www.tecmundo.com.br/seguranca/226937-porto-seguro-sofre-tentativa-ataque-hacker-afeta-sistemas.htm
Comercio		X									Atento Brasil S.A.	Compañía de servicios de relación con clientes y externalización de procesos de negocio incluyendo servicios de atención al cliente, de gestión de ventas y cobros, back office y soporte técnico	X	X		Ransomware-Lockbit 2.0	17/10/2021	Inhibición de acceso a las bases de datos y canales de comunicación	Afectó el funcionamiento de los call center operados por la compañía	46,1 millones de dólares, en concepto de lucro cesante provocado a las empresas clientes de los servicios prestados por Atento S.A.		46 100 000	Recuperación de la configuración desde copias de respaldo	https://www.convergenciadigital.com.br/Seguranca/Ataque-hacker-custou-R%24-230-milhoes-a-Atento-Brasil-60195.html?UserActiveTemplate=mobile
Estado		X									Ministerio de Salud	Máximo órgano de la Administración Federal encargado de la Salud pública y de su mantenimiento en el país	X	X		Ransomware	10/12/2021	El ataque fue realizado por "Lapsus Group" que asumió la autoría del delito con un mensaje que dejó publicado en las páginas y que decía "contáctennos si quieren recuperar los datos" y que "50 TB de datos habían sido copiados y excluidos"	Comprometió el sistema de notificación del Programa Nacional de Inmunizaciones y características técnicas que impiden la emisión del Certificado Nacional de Vacunación contra la covid-19, entre otros	Con los daños causados por el ataque, millones de brasileños quedaron imposibilitados de expedir el pasaporte digital de vacunación anticovid			Recuperación desde copias de respaldo	https://www.swissinfo.ch/spa/coronavirus-brasil_ataque-inform%C3%A1tico-al-ministerio-de-salud-de-brasil-bloquea-informaci%C3%B3n-covid/47182450

Tipo de actividad	Argentina	Brasil	Chile	Colombia	Ecuador	México	Panamá	Perú	Rep. Dominicana	Uruguay	Organización afectada	Descripción de la actividad	Impacto D	Impacto C	Impacto I	Tipo de incidente	Fecha de referencia del incidente	Descripción del incidente	Impacto Cualitativo	Impacto Cuantitativo	Impacto Días impacto	Impacto Costo en dólares	Resolución	Fuente
Estado		X									Policía Federal/ Policía Federal de Caminos	Servicio de policía	X	X		Ransomware	10/12/2021	Fue borrada información de agentes y de conductores	El ataque impactó el trabajo de miles de policías en todo el país, en especial aquellos que trabajan en el área administrativa y necesitan recabar información para encaminar acciones, investigaciones e inspección de entradas y personas en todo el país	No ponderado			Recuperación de la configuración desde copias de respaldo	https://www.correiodopovo.com.br/not%C3%ADcias/pol%C3%ADcia/ataque-hacker-derruba-sistemas-e-exclui-dados-da-pf-e-prf-1.743865
Educación		X									Instituto Federal de Paraná-IFPR	Educación terciaria. Cursos técnicos integrados y técnicos superiores	X	X		Ransomware	10/12/2021	El ataque consistió en borrar todos los sistemas, archivos y datos del ambiente institucional en la nube, con esto fue necesario realizar la recuperación de respaldos de bases de datos e instancias del sistema	El ataque al entorno de la nube que aloja los sistemas fue de un nivel de gravedad importante, habiendo inhibido totalmente el acceso a los servicios	Afectó la totalidad de los servidores, bases de datos y aplicaciones de la institución	7		Recuperación desde copias de respaldo	https://www.bemparana.com.br/noticia/instituto-federal-do-parana-confirma-ter-sido-alvo-de-hackers-na-ultima-sexta-feira
Educación		X									Instituto Federal de Piuaí	Educación terciaria. Cursos técnicos integrados y técnicos superiores	X	X		Ransomware	10/12/2021	El ataque consistió en borrar todos los sistemas, archivos y datos del ambiente institucional en la nube	Fue afectada toda la información administrativa y académica de la institución	No ponderado			Recuperación de la configuración desde copias de respaldo	https://www.otempo.com.br/politica/ataque-hacker-afetou-outros-orgaos-do-governo-federal-1.2582737
Estado		X									Alcaldía de Rio de Janeiro	Gobierno de nivel regional	X	X			10/12/2021	El ataque involucró a la mayoría de las aplicaciones del gobierno a excepción de las áreas de salud						https://www.cnnbrasil.com.br/nacional/ataque-hacker-tira-do-ar-sistemas-da-prefeitu rado-rio-de-janeiro/
Transporte		X									Urbanização de Curitiba S.A.	Transporte público de la ciudad de Curitiva	X	X		Ransomware	2/3/2022	El ataque afectó al sistema de recarga de la tarjeta de transporte pues 148 de las 254 líneas urbanas que integran el sistema tienen pago exclusivo de la tarjeta de transporte	Afectó principalmente a los estudiantes que necesitaban hacer o actualizar sus pases escolares y pagar la mitad de la tarifa	No ponderado	1		La empresa recomendó realizar compras de tarjetas de manera presencial en los puntos de venta habilitados	https://brasiline.com.br/blog/ciberataque-trava-transporte-publico-de-curitiba/
Estado		X									Servicio Municipal de Agua y Alcantarillado de Rio Grande do Sul	Servicios de provisión de agua potable y desagote de aguas servidas	X	X		Ransomware	3/7/2022	Interrupción en los sistemas, además de impactos en servicios, cambios de titularidad de los domicilios, acceso a registros, solicitudes de tarifas de la seguridad social y la inspección local	Durante el ataque a la red, los datos y los archivos se dañaron, incluidas las copias de seguridad, fueron secuestrados. Debido a esto, el acceso a documentos importantes en las áreas, como proyectos de ingeniería, es inaccesible	100% de los servicios y gestiones de la empresa			Recuperación de la configuración desde copias de respaldo	https://www.securityreport.com.br/destaques/semae-sofre-ataque-cibernetico-em-sistemas/
Estado		X									Alcaldía de Rio de Janeiro	Gobierno de nivel regional	X	X		Ransomware	16/8/2022	La alcaldía no informó en detalle sobre los niveles de afectación involucrados	El ataque involucró a la mayoría de las aplicaciones del gobierno a excepción de las áreas de salud y otras aplicaciones	No ponderado			Recuperación paulatina de configuraciones y datos, desde copias de respaldo	https://www.cnnbrasil.com.br/nacional/ataque-hacker-tira-do-ar-sistemas-da-prefeitura-do-rio-de-janeiro/

Tipo de actividad	Argentina	Brasil	Chile	Colombia	Ecuador	México	Panamá	Perú	Rep. Dominicana	Uruguay	Organización afectada	Descripción de la actividad	Impacto D	Impacto C	Impacto I	Tipo de incidente	Fecha de referencia del incidente	Descripción del incidente	Impacto Cualitativo	Impacto Cuantitativo	Impacto Días impacto	Impacto Costo en dólares	Resolución	Fuente
Tecnología		X									Página oficial de Jail Bolsonaro (candidato oficialista a presidente (elecciones 2022)	Página de campaña política			X	Defacement (ataque de desfiguración)	31/8/2022	El ataque modificó la información del sitio web sin alterar las direcciones del mismo, por lo que cualquiera que entre en la web de manera normal verá los mensajes que dejaron los atacantes	No especificado	No especificado			Recuperación de la configuración desde copias de respaldo	https://www.cronista.com/infotechnology/actualidad/elecciones-brasil-2022-hackearon-la-pagina-de-jair-bolsonaro/
Tecnología			X								Bell y Cía.	Estudio jurídico	X	X		Ransomware	1/1/2021	Secuestro del sitio web de la empresa. Según reconocieron los propios afectados, alojaba información privilegiada y datos sensibles de sus clientes	El ataque provocó un alto nivel de perjuicio en la reputación de la empresa	Rescate solicitado de u$s 4200		4 200	No informado	https://www.americaeconomia.com/empresas-ciberataque-de-latinoamerica-crece
Energía			X								Empresa Nacional del Petróleo-ENAP	Empresa estatal chilena dedicada a la explotación, producción, refinación y comercialización de petróleo y sus derivados		X	X	Filtración de información reservada/ phishing/ Ingeniería social	1/2/2021	Filtración de los sistemas informáticos de la empresa, que permitió acceder a información reservada utilizada (una conversación y cadena de mensajes legítima) para originar una gestión bancaria (transferencia de fondos) que sería el medio para concretar el fraude. La operación se abortó gracias al aviso de la entidad bancaria involucrada (involuntariamente) en la estafa	Se vulneraron los sistemas informáticos de la ENAP y accedió a información secreta de la firma estatal	No informado			Reconfiguración de las cuentas de correo electrónico afectadas	https://www.biobiochile.cl/especial/bbclinvestiga/noticias/reportajes/2022/08/14/hackers-violan-sistemas-de-enap-y-acceden-a-informacion-secreta-en-intento-de-fraude-internacional.shtml
Tecnología			X								SITA	Firma proveedora de servicios de comunicación y tecnología de información para la industria aérea		X		Filtración de datos	24/2/2021	Exfiltración de datos desde los servidores en que se almacena su servicio SITA Passenger Service System (PSS)	Los datos exfiltrados son nombres de clientes, status en sus programas de viajero frecuente y número de membresía	Algunas de las firmas que han revelado ser parte de la brecha de seguridad en los sistemas de SITA son American Airlines, British Airways, Lufthansa, Air New Zealand, Finnair, Singapore Airlines, Malaysia Airlines, Aegean y Jeju Air			Algunas empresas recomendaron a sus clientes cambiar sus credenciales de acceso a sus portales web	https://www.csirt.gob.cl/noticias/sita/
Industria			X								Atacama Minerals Chile S.C.M.	Subsidiaria de la minera de Vancouver Atacama Minerals Corp. La compañía posee el 100% del depósito de yodo, sulfatos y nitratos Aguas Blancas	X	X		Ransomware	1/1/2022	Usurpación de los sistemas informáticos del departamento de finanzas y cifraron todos los datos sin que la empresa pudiera acceder a la información	No informado	No informado			No informado	https://www.bnamericas.com/es/noticias/tecnologias-de ciberseguridad-se-estarian-quedando-obsoletas
Estado			X								Departamento de Informática del Poder Judicial	Servicio interno de tecnología informática	X	X		Ransomware-LockBit	16/9/2022	El organismo confirmó que un pequeño porcentaje de computadoras de la institución que utilizan Windows 7 fueron comprometidas con un ransomware que cifró los archivos	Funcionarios de la Corte de Apelaciones de Santiago comenzaron a reportar que sus computadoras estaban funcionando mal	Aproximadamente 150 computadoras conectadas a la red corporativa fueron infectadas			Actualización del sistema operativo de los equipos afectados	https://www.elperiodista.cl/2022/09/conoce-mas-sobre-el-ataque-del-ransomware-lockbit-que-afecto-al-poder-judicial/

Tipo de actividad	Argentina	Brasil	Chile	Colombia	Ecuador	México	Panamá	Perú	Rep. Dominicana	Uruguay	Organización afectada	Descripción de la actividad	Impacto D	Impacto C	Impacto I	Tipo de incidente	Fecha de referencia del incidente	Descripción del incidente	Impacto Cualitativo	Impacto Cuantitativo	Impacto Días impacto	Impacto Costo en dólares	Resolución	Fuente
Estado			X								Estado Mayor Conjunto de las fuerzas armadas-EMCO	Organismo de trabajo y asesoría permanente del Ministro de Defensa de Chile		X		Filtración de base de datos de correo electrónico	22/9/2022	Secuestro de información sensible con el objeto de exponerla en Internet	Los correos electrónicos que fueron expuestos incluyen documentos rotulados como "reservado", "secreto" y "ultra -secreto", de áreas sensibles de la defensa, como la estrategia de ciberseguridad, el sistema de monitoreo de comunicaciones satelitales en las fronteras y programas para almacenar bases de datos de inteligencia	En total, se expusieron más de 400 mil mensajes enviados y recibidos por esas casillas entre 2012 y mayo de 2022, aunque la mayoría se concentran desde 2018 en adelante. La información suma 340 gigabytes	9		No informado	https://www.ciperchile.cl/2022/09/22/hackeo-masivo-al-estado-mayor-conjunto-expuso-miles-de-documentos-de-areas-sensibles-de-la-defensa/#:~:text=El%2017%20de%20junio%20de,forma%20permanente%2024%2F7%E2%80%9D
Finanzas			X								Binance Exchance (plataforma de criptomonedas)	Intercambio de criptomonedas en términos de volumen de comercio			X	Robo de criptomoneda	7/10/2022	Robo de "tokens" de un puente de blockchain utilizado en la cadena	Grave falla en la administración de la ciberseguridad, habida cuenta que a la fecha del incidente ya se habían registrado 13 incidentes de estas características a nivel mundial	Robo de u$ 570 millones en bitcoins		570000000	No informado	https://www.df.cl/mercados/divisas/hackeo-de-criptomonedas-golpea-a-blockchain-vinculada-a-binance
Comercio				X							Mundial de Repuestos	Empresa de actividad comercial de repuestos de Bogotá			X	Violación a la seguridad del PBX	1/11/2020	Empresa de repuestos de Bogotá fue víctima de un ciberataque generando cargos por llamadas telefónicas internacionales	Los vectores de ataque más usados incluyen: La recopilación de información, enumeración de extensiones, escucha clandestina, manipulación telefónica, ataques de autenticación y la suplantación de identidad, y ataques de denegación de servicio	Aumento desmedido del tráfico de llamadas telefónicas internacionales		35 000	No informada	https://www.itechsas.com/blog/ciberseguridad/empresa-de-bogota-debera-pagar-factura-por-160-millones-al-descubrir-que-fue-hackeada/
Educación				X							Universidad El Bosque	Educación superior	X	X	X	Acceso a cuentas y contraseñas de servidores de correo y usuarios de ciertas redes públicas	12/8/2021	Se habrían registrado vulnerabilidades identificadas que no habían sido aseguradas	Imposibilidad del acceso a las cuentas de correo electrónico, información en la nube, calificaciones, documentos administrativos y afines	A la totalidad de los usuarios de las distintas aplicaciones afectadas			Recurrir a las cadenas de WhatsApp y su página de Facebook para tener alguna comunicación con su comunidad académica	https://es.linkedin.com/pulse/ciberseguridad-en-colombia-2021-seis-ataques-y-jeimy-cano-ph-d-cfe

Tipo de actividad	Argentina	Brasil	Chile	Colombia	Ecuador	México	Panamá	Perú	Rep. Dominicana	Uruguay	Organización afectada	Descripción de la actividad	Impacto D	Impacto C	Impacto I	Tipo de incidente	Fecha de referencia del incidente	Descripción del incidente	Impacto Cualitativo	Impacto Cuantitativo	Impacto Días impacto	Impacto Costo en dólares	Resolución	Fuente
Estado				X							Empresas Públicas de Cali-EMCALI	Empresa prestadora de servicios públicos (energía, acueducto, alcantarillado y telecomunicaciones)	X	X		Ransomware	12/8/2021	Servidores encriptados con contraseña	El virus entró por un equipo que hace parte de una red interconectada que tiene carpetas compartidas, por lo que resultaron encriptados, y de más información valiosa. Además, algunos clientes recibieron un correo a nombre de Emcali con contenido adjunto que era el mismo virus, buscando que fueran descargados para robar datos de los usuarios	Cerca de 28.000 equipos (*routers*) usados por la empresa para brindar el servicio de Banda Ancha a sus clientes se vieron afectados por este problema		100 000	No informado	https://es.linkedin.com/pulse/ciberseguridad-en-colombia-2021-seis-ataques-y-jeimy-cano-ph-d-cfe
Estado				X							Alcaldía de Santa Fe de Antioquia	Gobierno de nivel regional	X	X		Ransomware	19/8/2021	Fueron secuestrados datos, documentos e información financiera del municipio, por lo que las cuentas bancarias permanecen congeladas, así como algunos trámites que realizaba la Secretaría de Hacienda	El ataque imposibilitó la continuidad operativa informática de la alcaldía	Bloqueo de todos los servicios de la institución, afectando también todo el tema de cuentas bancarias			No informado	https://www.infobae.com/america/colombia/2021/08/19/ciberdelincuentes-secuestraron-los-datos-de-la-alcaldia-de-santa-fe-de-antioquia/
Estado				X							Unidad Administrativa Especial de Aeronáutica Civil	Organismo estatal encargado del control y regulación de la aviación civil		X	X	Phishing	31/8/2021	Perjudicar los servidores internos de la autoridad aérea	Preventivamente se suspendieron los servicios internos como el correo electrónico, la intranet y página web de la entidad. De esta forma, se aseguró frenar la propagación del ataque		3		Aeronáutica Civil no reveló más detalles acerca del ataque	https://www.infobae.com/america/colombia/2021/09/01/la-aeronautica-civil-confirmo-ataque-cibernetico/
Estado				X							Departamento Administrativo Nacional de Estadística-DANE	Entidad responsable de la producción de estadísticas oficiales en Colombia, así como de la coordinación del Sistema Estadístico Nacional	X	X	X	Ransomware	9/9/2021	Indisponibilidad de la información albergada en los servidores del Dane, así como problemas en las aplicaciones para la recolección y producción estadística, en el correo Zimbra, el sistema Orfeo, los servidores de procesamiento estadístico, los antivirus, los servidores de aplicación como apache, el de back up, el de almacenamiento de archivos y el de impresiones	Alto, afectando la operación del DANE a nivel nacional. Se cayó la página web, el correo electrónico institucional, se borraron sistemas de procesamiento estadístico, bases de datos, (que contiene información de carácter reservado y con información sensible y confidencial). Tenemos logs que dan cuenta de la posible eliminación del respaldo y la afectación de aproximadamente de 420 servidores. Afectando 130 tb de información	Se estiman afectados 130tb de datos		25 000	No informado	https://www.infobae.com/america/colombia/2021/11/12/dane-radico-denuncia-penal-contra-atacantes-de-sus-plataformas-digitales/

Tipo de actividad	Argentina	Brasil	Chile	Colombia	Ecuador	México	Panamá	Perú	Rep. Dominicana	Uruguay	Organización afectada	Descripción de la actividad	Impacto D	Impacto C	Impacto I	Tipo de incidente	Fecha de referencia del incidente	Descripción del incidente	Impacto Cualitativo	Impacto Cuantitativo	Impacto Días impacto	Impacto Costo en dólares	Resolución	Fuente
Educación				X							Pontificia Universidad Javeriana	Educación superior	X	X	X	Intento de filtración	23/11/2021	Fueron detectados intentos de acceso a los servidores de la institución, en las sedes de Bogotá y Cali. No encontrándose evidencia fuga o pérdida de información por el ataque	La universidad deshabilitó algunos servicios tecnológicos para proteger la operación informática	No aplica			Recuperación paulatina de configuraciones y datos, desde copias de respaldo	https://www.semana.com/nacion/articulo/la-universidad-javeriana-confirma-que-sufrio-ataque-informatico-en-bogota-y-cali/202153/
Estado				X							Instituto Nacional de Vigilancia de Medicamentos y Alimentos-INVIMA	Institución de referencia nacional en materia sanitaria y ejecutar las políticas formuladas por el Ministerio de Salud y Protección Social en la inspección, vigilancia y control de calidad de los medicamentos, productos biológicos, alimentos, bebidas, cosméticos, dispositivos y otros	X	X		Ransomware-Blackbyte	7/3/2022	Los atacantes ganaron acceso al servidor gracias a una vulnerabilidad de Microsoft Exchange Server, que permite acceder a los recursos hasta ganar privilegios de administrador	Invima queda imposibilitado de ejercer su función de control, quedando detenida la mercadería de ingreso/egreso	Se produjo la no disponibilidad de información y de los aplicativos externos, a excepción de la Ventanilla Única de Comercio Exterior (VUCE)	22		Durante la duración del ataque se pasó a operación manual apoyado en resoluciones de emergencia tomadas por el Gobierno	https://consultorsalud.com/invima-objeto-ataque-cibernetico/
Varias				X							Por las características del ataque, fueron afectadas distintas organizaciones	Industrias, organizaciones con y sin fines de lucro, y entidades gubernamentales.		X	X	Phishing-troyano (njRAT)/ Control remoto de los equipos afectados	18/5/2022	Acceso remoto y persistir en el equipo comprometido sin ser detectado el mayor tiempo posible. Este código malicioso permite a los atacantes controlar el equipo infectado de manera remota y realizar acciones como enviar y recibir archivos, registrar las pulsaciones del teclado, hacer capturas de pantalla, tomar imágenes con la cámara y registrar audio, entre muchas otras	En el caso de los usuarios domésticos, la infección puede conllevar la pérdida de información relativamente poco importante que se puede reemplazar fácilmente, o bien, generar pérdida de información que ofrece al cibercriminal acceso a la cuenta bancaria del usuario. En una red corporativa, el virus troyano que envía spam puede generar un leve aumento del tráfico de comunicación, en tanto que otros tipos de infección pueden causar el colapso total de la red corporativa o la pérdida de datos críticos de la empresa	Indeterminado			La aplicada por cada organización comprometida	https://prensariotila.com/operacion-discordia-eset-descubre-una-campana-de-espionaje-en-colombia/
Organización no gubernamental				X							Fundación Paz y Reconciliación	Organización sin fines de lucro	X	X		Robo de información-pishing	9/8/2022	La entidad contaba con informes, notas, columnas y artículos en más de 5.000 entradas, de índole política, en su página web	El organismo identificó la pérdida de información no pudiendo tomar acciones al respecto	Pérdida de material académico, estimado en 5.000 publicaciones			No informado	https://www.infobae.com/america/colombia/2022/08/10/fundacion-pares-denuncia-que-fue-victima-de-un-ataque-cibernetico-borraron-cerca-de-5000-entradas-investigativas/

Tipo de actividad	Argentina	Brasil	Chile	Colombia	Ecuador	México	Panamá	Perú	Rep. Dominicana	Uruguay	Organización afectada	Descripción de la actividad	Impacto D	Impacto C	Impacto I	Tipo de incidente	Fecha de referencia del incidente	Descripción del incidente	Impacto Cualitativo	Impacto Cuantitativo	Días impacto	Costo en dólares	Resolución	Fuente
Estado					X						Corporación Nacional de Telecomunicaciones-CNT EP	Empresa estatal de telecomunicaciones ecuatoriana creada el 30 de octubre de 2008; opera servicios de telefonía fija local, regional e internacional, acceso a internet estándar y de alta velocidad (Dial UP, DSL, Internet móvil 3G y 4G LTE), televisión satelital y telefonía móvil	X	X		Ransomware-RansomEXX	22/7/2021	La empresa había señalado que sus sistemas registraban intermitencias en sus sistemas de atención al cliente, agencias y Contact Center. Informando luego haber sufrido un ataque informático de tipo ransomware	Afectó el funcionamiento de áreas como facturación, activaciones y recargas	La empresa anunció la afectación de 11,23 giga bytes. Según dijo el grupo de ciberdelincuentes inicialmente, habrían podido descargar 190 gigabytes en archivos internos de la compañía de telecomunicaciones			No informado. Se presume recuperación de configuraciones y datos desde copias de resguardo	https://www.elcomercio.com/actualidad/negocios/virus-ransomeware-cnt-ministerio-telecomunicaciones.html
Estado					X						Consejo de Comunicación	El Consejo es una institución encargada de regular, desarrollar y promocionar el ejercicio de la comunicación y la información con enfoque en los Derechos Humanos	X	X		Ransomware	3/8/2021	Encriptación de las bases de datos, luego de identificado el ataque se apagaron los servidores. Ante las acciones de la institución para salvaguardar la información tuvieron que aislar, contener y erradicar, para luego sanear el sistema	Preventivamente se desconectaron todos los servicios del consejo	Debido a la incidencia del ataque y a las acciones preventivas adoptadas por el consejo, este permaneció inactivo durante el tiempo que demandó el saneamiento de los servicios	1		Recuperación paulatina de configuraciones y datos, desde copias de respaldo	https://www.infobae.com/america/america-latina/2021/08/04/nuevo-ataque-ciberneticoa-un-organismo-estatal-ecuatoriano/
Finanzas					X						Banco Pichincha	Actividad financiera	X	X		Ransomware-Cobalt Strike	9/10/2021	Se interrumpió las operaciones, y dejó fuera de servicio algunas funcionalidades de los cajeros automáticos y el portal de banca online	Se desconectaron servidores que pudieran estar potencialmente afectados del resto de la red	Indeterminado debido a las características selectivas del ataque	1		Recuperación paulatina de configuraciones y datos, desde copias de respaldo	https://www.cronista.com/infotechnology/actualidad/el-peligro-virus-que-atac-a-un-banco-de-ecuador-puede-llegar-ac/
Estado					X						Agencia Nacional de Tránsito-ANT	Agencia dedicada a contribuir al desarrollo del país a través de la planificación, regulación y control del transporte terrestre			X	Tipo de ataque no confirmado	21/10/2021	El incidente obligó a sacar de servicio al sistema AIX (software de gestión de vídeo), utilizado para el registro de multas de tránsito, consultado para la renovación de licencias de conducir	Fueron afectados el almacenamiento de los datos de matriculación, licencia y otros procesos de la ANT	Indeterminado, de acuerdo a la cantidad de turnos reprogramados luego de la normalización de los servicios			No informado. Se presume recuperación de configuraciones y datos desde copias de resguardo	https://gk.city/2021/10/21/sistema-ant-ataque-informatico/
Finanzas						X					Banco de México -BANXICO	Actividad financiera			X	Degradación del servicio en su página Web	7/7/2020	Degradación de los servicios e intento de hackeo en su página Web	Los mecanismos y protocolos de protección establecidos por el Banco de México para este tipo de circunstancias evitaron afectaciones a sus procesos en los mercados financieros y sistemas de pagos	Indeterminado por las características del ataque	1		Debido a los monitoreos permanentes con los que cuenta la institución, se logró activar los mecanismos de defensa y con esto, detener el ataque	https://www.infobae.com/america/mexico/2020/07/08/el-banco-de-mexico-reporto-intento-de-hackeo-a-su-pagina-web/

Tipo de actividad	Argentina	Brasil	Chile	Colombia	Ecuador	México	Panamá	Perú	Rep. Dominicana	Uruguay	Organización afectada	Descripción de la actividad	Impacto D	Impacto C	Impacto I	Tipo de incidente	Fecha de referencia del incidente	Descripción del incidente	Impacto Cualitativo	Impacto Cuantitativo	Días impacto	Costo en dólares	Resolución	Fuente
Estado						X					Lotería Nacional para la Asistencia Pública	Institución del gobierno de México encargada de realizar juegos y sorteos legales en el país	X	X		Ransomware-Avaddon	14/5/2021	Secuestro de miles de datos en 2021, debido a la obsolescencia de equipos y a sus sistemas vulnerables sin actualizaciones de seguridad	Fueron secuestrados datos como contratos y convenios de 2009 a 2021, documentos legales, correspondencia, finanzas, datos notariales, outsourcing, y mucho más	$ 4.479.000 (mexicanos), estimados por la Auditoría Superior de la Federación	77	230 000	No informada	https://www.animalpolitico.com/2022/07/lotenal-ataque-ciberneticos-obsolencia-equipos/
Estado						X					Instituto Nacional de Acceso a la Información-INAI	Organismo público autónomo encargado de facilitar y garantizar el acceso de las personas a la informa-ción pública y el acceso y protección de los datos personales, promover la cultura de la transparencia en la gestión pública y la rendición de cuentas del gobierno a la sociedad			X	Cripto minería	21/9/2021	De abril del 2019 a septiembre del 2020, la dependencia registró 2 millones 973 mil 954 “peticiones maliciosas”	INAI no aclara qué servicios fueron vulnerados, sin embargo, aclara que fue un “ataque o hackeo de tipo de explotación de criptomonedas”	INAI no informo sobre el impacto cuantitativo del ataque	540		INAI no reveló más detalles acerca del ataque	https://www.infobae.com/america/mexico/2021/09/21/millones-de-ciberataques-al-inai-en-ano-y-medio-segun-solicitud-de-informacion-de-la-onea/
Industria						X					Bridgestone Latinoamérica Sur	Bridgestone Latinoamérica Sur cuenta con equipos en Brasil, Argentina y Chile con cinco plantas de producción, que producen neumáticos de pasajeros, comerciales y agrícolas, así como bandas de rodamiento Bandag	X	X		Ransomware	27/2/2022	Entre fines de febrero y principios de marzo se detectó "un incidente de seguridad informática" el 27 de febrero y rápidamente desconectó los sistemas afectados del resto de su red. Una vez contenida la amenaza, el grupo pudo reconectar sus sistemas y devolver progresivamente a la actividad normal	La empresa inactivó la totalidad de sus servidores	La empresa no detalló el impacto productivo del ataque	10		La empresa no reveló más detalles acerca del ataque	https://www.eleconomista.com.mx/empresas/Ciberataque-contra-Bridgestone-freno-una-semana-su-produccion-de-neumaticos-en-America-20220318-0025.html
Industria						X					Foxconn	Proveedor internacional de semiconductores y otros productos electrónicos	X	X		Ransomware-grupo LockBit	31/5/2022	Habría afectado la operación de la unidad, el atacante dio como fecha límite el 11 de junio para que Foxconn se comunique y pague el rescate; de lo contrario, los archivos confidenciales de la compañía se harán públicos; sin embargo, no hay información sobre lo que estaría en posesión de los bandidos y la cantidad que se le estaría pidiendo a la empresa	La empresa no detalló sobre el alcance del ataque	La empresa no detalló sobre el alcance del ataque			No informado	https://canaltech.com.br/seguranca/ransomware-atinge-fabrica-da-foxconn-no-mexico-217876/
Estado							X				Ministerio de Desarrollo Social de Panamá-MIDES	Este ministerio se encarga de las situaciones sociales de la República de Panamá	X	X		Ransomware	9/1/2021	Varios equipos fueron atacados inhabilitando varios servidores, entre los cuales está el Registro Nacional de Beneficiarios	El ataque afectó la infraestructura de red dejando fuera de servicio varios servidores e inhabilitando los sistemas de respaldo	No informado			MIDES no reveló más detalles acerca del ataque	https://www.welivesecurity.com/la-es/2021/01/12/ataque-ransomware-afecta-ministerio-desarrollo-social-panama/

Tipo de actividad	Argentina	Brasil	Chile	Colombia	Ecuador	México	Panamá	Perú	Rep. Dominicana	Uruguay	Organización afectada	Descripción de la actividad	Impacto D	Impacto C	Impacto I	Tipo de incidente	Fecha de referencia del incidente	Descripción del incidente	Impacto Cualitativo	Impacto Cuantitativo	Impacto Días impacto	Impacto Costo en dólares	Resolución	Fuente
Logística							X				Aeropost, Inc.	Empresa de comercio electrónico y logística que opera el sitio web Aeropost.com		X		Violación de datos de los clientes	24/4/2022	La empresa confirmó que hubo una brecha de datos de corta duración en la plataforma tecnológica operada por Aeropost, lo que resultó en que algunas tarjetas de crédito de los clientes se vieran comprometidas	Evidencia de fallos en los niveles de seguridad de datos y de la *tokenización* de todas las tarjetas	Indeterminado por las características del ataque			La empresa comunica a sus clientes que cancele las operaciones realizadas a través de las respectivas entidades emisoras	https://www.jdsupra.com/legalnews/aeropost-com-asks-customers-to-delete-4835917/
Estado								X			Ministerio de Transportes y Comunicaciones	Órgano que busca lograr un racional ordenamiento territorial vinculado a las áreas de recursos, producción y mercados		X	X	Secuestro de la cuenta de Twitter	29/3/2022	La cuenta de Twitter del Ministerio ha sido secuestrada y rebautizada como MTC.ETH	Se presume que pudo haber quedado expuesta información personal de ciudadanos que, por una gestión, pudieron compartir números de documentos y teléfonos	La cuenta tiene aproximadamente 260 mil seguidores	1		No informado	https://rpp.pe/tecnologia/redes-sociales/twitter-cuenta-secuestrada-del-mtc-luce-un-bored-ape-como-avatar-noticia-1396019
Estado								X			Dirección General de Inteligencia del Ministerio del Interior-Digimin	La Dirección General de Inteligencia del Ministerio del Interior DIGIMIN coordina y centraliza la inteligencia relacionada al orden interno, seguridad pública, seguridad ciudadana, crimen organizado y nuevas amenazas transnacionales, que produce la Dirección de Inteligencia de la Policía Nacional	X	X		Ransomware-grupo Conti-Secuestro de información sensible	28/4/2022	El atacante asegura haber penetrado en los servidores de la Digimin y secuestrados documentos secretos de una oficina que es estratégica para la seguridad nacional. Exigen dinero al Estado peruano a cambio de no publicar la información	Información altamente sensible del organismo	No se publicó el volumen de los datos afectados			No informado	https://sudaca.pe/noticia/informes/hackers-rusos-en-los-servidores-de-inteligencia-del-mininter/
Estado									X		Contraloría General de la República Dominicana	Órgano Rector del Sistema Nacional de Control Interno de la República Dominicana	X			Defacement-Bloqueo de la página Web	6/2/2022	Un supuesto grupo paquistaní hackeó la mañana de este domingo la página virtual de la Contraloría General de la República Dominicana, por lo que las personas no pueden acceder a la misma ni visualizar nada de la institución	Bloqueo total del acceso a la información	No se ha informado el volumen de los datos afectados			No informado	https://encontexto.com.do/hackean-pagina-de-la-contraloria-general-de-la-republica-dominicana/
Estado									X		Consejo Estatal del Azúcar	Organismo que administra los ingenios y la producción de azúcar en la República Dominicana bajo la Dirección General de Bienes Nacionales	X			Defacement - Bloqueo de la página Web	6/2/2022	Desconfiguración de la estructura web	Bloqueo total del acceso a la información	No se ha informado el volumen de los datos afectados			No informado	https://www.gadgetdominicana.com/2022/02/14-sitios-web-del-estado-dominicano-hackeados-estn-en-peligro-los-datos-de-los-ciudadanos/
Estado										X	Usuarios particulares en general	La propia de cada usuario	X	X	X	Ransomware-Troyano identificado como "Ministerio del Interior de Uruguay"	1/12/2020	Es parte de una estafa en línea conocida que se utiliza para robar dinero de usuarios de computadoras ubicados en Uruguay	Intenta convencer a sus víctimas de que están siendo procesadas por actividades ilegales en línea y luego exige el pago de una multa policial falsa	Variable según las víctimas afectadas			No aplica	https://www.enigmasoftware.com/ministeriointerioruruguayvirus-removal/

Tipo de actividad	Argentina	Brasil	Chile	Colombia	Ecuador	México	Panamá	Perú	Rep. Dominicana	Uruguay	Organización afectada	Descripción de la actividad	Impacto D	Impacto C	Impacto I	Tipo de incidente	Fecha de referencia del incidente	Descripción del incidente	Impacto Cualitativo	Impacto Cuantitativo	Impacto Días impacto	Impacto Costo en dólares	Resolución	Fuente
Estado										X	Dirección Nacional de Identificación Civil	Organismo que se encarga de la identificación de las personas físicas que habitan el territorio		X	X	Robo y alteración de los datos	8/12/2020	No fueron informados los aspectos técnicos del ataque, pero sí que el mismo vulneró los datos de cierta cantidad de pasaportes electrónicos, comprometiendo información sensible que incluye datos biométricos de las personas: fotografía, huella digital, nombre y número de documento de identidad	Alteración de datos de alta sensibilidad	Afectó 84.001 pasaportes electrónicos	45		El organismo no informó detalles técnicos	https://www.derechosdigitales.org/19045/pasaportes-hackeados-respuestas-insuficientes-y-datos-vulnerados/
Estado										X	Armada Nacional	La Armada Nacional de la República Oriental de Uruguay es el nombre dado a la marina de guerra de la República Oriental del Uruguay	X	X		Correo electrónico con datos de cuentas de usuarios internos	18/1/2021	Se identificó un correo electrónico externo remitido a la institución, marcado como spam y con formato de mensaje interno, que contenía datos sobre cuentas de correo, nombres de usuarios y contraseñas	Preventivamente se inactivó la red de internet e intranet de la fuerza, que derivó en que se quedaran sin correo electrónico	El correo en cuestión contenía la información de al menos 50 usuarios	1		No informado	https://www.visionmaritima.com.uy/noticias/actualidad-noticias/investigan-ciberataque-inedito-contra-al-menos-50-cuentas-de-mail-de-la-armada/
Tecnología										X	Administración Nacional de Telecomunicaciones	Compañía estatal de telecomunicaciones de telefonía móvil, fija y de las conexiones a internet por cable, contando con el monopolio de estas dos últimas		X		Robo de datos de clientes	3/10/2021	Filtración de datos de clientes de la empresa	La lista de nombres y apellidos sobre los que hay información variada (fechada hasta marzo de 2017). De algunos aparece su cédula de identidad, fecha de nacimiento y teléfono celular; de otros, sólo el documento, el mail o el género	La información filtrada corresponde aproximadamente a 100.000 clientes			No aplica	https://ladiaria.com.uy/politica/articulo/2021/10/hackers-aseguran-que-robaron-informacion-de-antel-pero-la-empresa-estatal-no-tiene-evidencia-de-ningun-evento-nuevo-de-ciberataque/
Estado										X	Administración Nacional de Combustibles Alcohol y Pórtland	Abastecimiento de productos energéticos y proveemos cementos pórtland y alcoholes,	X	X		Ransomware	29/4/2022	La compañía estatal uruguaya detectó la presencia de código malicioso en software utilizado para la distribución de combustible y monitoreo de vehículos oficiales. La amenaza estaba programada para ejecutarse más adelante	No aplica	No aplica			No aplica	https://www.welivesecurity.com/la-es/2022/04/29/ancap-detecta-malware-software-utilizado-distribucion-combustible/
Finanazas										X	Banco Santander	Banco comercial y de servicios financieros		X		Malware-troyano-vía correo electrónico	16/6/2022	Preventivamente el banco Santander con el respaldo del Banco de la República Oriental del Uruguay, advierte a sus clientes sobre la circulación de un malware tipo troyano que intenta instalarse en los equipos atacados con el objeto de secuestrar información sensible. Presentándose como un correo auténtico que contiene una descarga ejecutable	A la instalación del virus, este puede "mutar" a ransomware para el secuestro de información o bien suplantar la identidad del titular para enviar correos electrónicos a terceros, realizar operaciones bancarias o manejar sus redes sociales	Variable según las víctimas afectadas			No aplica	https://www.elobservador.com.uy/nota/brou-y-santander-advierten-sobre-un-troyano-que-puede-secuestrar-tu-informacion-202261611141

Tipo de actividad	Argentina	Brasil	Chile	Colombia	Ecuador	México	Panamá	Perú	Rep. Dominicana	Uruguay	Organización afectada	Descripción de la actividad	Impacto D	Impacto C	Impacto I	Tipo de incidente	Fecha de referencia del incidente	Descripción del incidente	Impacto Cualitativo	Impacto Cuantitativo	Días impacto	Costo en dólares	Resolución	Fuente
Tecnología			X			X					SolarWinds Corporation	Empresa estadounidense que desarrolla software para ayudar a las empresas a administrar sus redes, sistemas e infraestructura de tecnología de la información		X		Filtración de datos (puerta trasera)-Sunburst	13/12/2020	El ciberataque infectó a las actualizaciones de su software de monitoreo de redes Orion	SolarWinds solicitó, ese mismo día, a sus clientes actualizar Orion inmediatamente a su versión 2020. 2.1 HF 1	Se estima que fueron afectadas aproximadamente 18.000 empresas en todo el mundo	4		Aplicar una nueva actualización de emergencia, la que reemplazará el componente comprometido y agregará nuevas funcionalidades de seguridad	https://www.csirt.gob.cl/media/2020/12/10CND20-00045-01.pdf
Tecnología	X					X					Kaseya Limited	Servicios de TI	X	X		Ransomware-Revil	2/7/2021	Ataque contra el servicio VSA (software de gestión de IT) el ataque se llevó a cabo mediante la explotación de una vulnerabilidad zero-day (CVE-2021-30116)	Cerraron los servidores SaaS y notificaron el problema a los clientes para que apagaran los servidores VSA	Se estima que fueron afectadas aproximadamente 1500 empresas	4		La empresa desarrolló un parche de solución	https://www.xataka.com/seguridad/kaseya-su-espeluznante-ataque-ransomware-esto-todo-que-sabemos-momento
Tecnología				X				X			Securitas	Firma de vigilancia, seguridad y gestión de riesgos corporativos		X	X	Filtración de información reservada	31/1/2022	Uno de los tres buckets Amazon Simple Storage Service (AS3) de la firma estaba completamente expuesto en línea	La información expuesta incluye identificación personal de los empleados y detalles de las instalaciones de al menos cuatro aeropuertos	Filtración de más de 1 millón de archivos confidenciales, equivalentes a 3TB			No informado	https://noticiasseguridad.com/hacking-incidentes/filtran-informacion-personal-y-fotos-de-los-empleados-en-aeropuertos-de-colombia-y-peru/
Tecnología		X		X	X						Operadores de telecomunicaciones	Persona física o jurídica que explota redes públicas de telecomunicaciones o presta servicios de telecomunicaciones disponibles al público	X	X		Ransomware-LightBasin	Año 2021	El tráfico del malware emuló los servidores que manejan las conexiones GPRS, lo que le permitió enviar y recibir datos entre los sistemas infectados y los servidores de comando y control sin alertar al firewall	El procedimiento de los ataques fue el mismo: captura de la base de datos, un DDoS y pedido de rescate que debe ser depositado en billeteras virtuales	En octubre de 2021 fue anunciado, que las redes de 13 operadores globales de telefonía móvil fueron infiltradas	120	5 000 000	No informada	https://enperspectiva.uy/enperspectiva-net/gente-y-empresas/empresas-de-telecomunicaciones-recibieron-un-tercio-de-los-ata ques-ciberneticos-perpetrados-en-2021/
Tecnología		X		X		X					Por las características del ataque afectó a distintas entidades bancarias	Bancos comerciales y de servicios financieros		X	X	Troyano bancario-Qbot	8/1/2021	Distribución por correo electrónico del malware Qbot, con la finalidad de robar datos sensibles de las redes empresariales infectadas	No fue difundido por los distintos usuarios afectados	1.500 usuarios afectados en distintos países	90		El 22 de marzo, Microsoft anunció que en el 92% de los servidores in situ de Microsoft Exchange, los efectos del hackeo habían sido corregidos o mitigados	https://portalinnova.cl/nueva-ola-de-correos-maliciosos-propaga-el-malware-qbot-advierte-kaspersky/
Logística						X		X	X		Expeditors International	Empresa estadounidense de logística y transporte de carga con filiales en distintos países del mundo. Sus servicios incluyen la cadena de suministro, el almacenamiento y la distribución, el transporte, las aduanas y el cumplimiento	X	X		Ransomware	20/2/2022	La compañía de logística y transporte de mercancías debió cerrar la mayor parte de sus operaciones en todo el mundo para mantener "la seguridad de su entorno global de sistemas"	Los impactos en curso del ciberataque tuvieron un efecto material adverso en su negocio, ingresos, gastos, resultados de las operaciones, flujos de efectivo y reputación. En un principio, la empresa no puede estimar las repercusiones financieras directas e indirectas definitivas de este ciberataque	La empresa tiene 350 sucursales y más de 18.000 empleados en todo el mundo			Se aplicaron soluciones de contingencia de acuerdo a cada filial y disponibilidad de recursos	https://www.baenegocios.com/negocios/Un-ciberataque-obligo-a-un-gigante-logistico-a-cerrar-sus-operaciones-mundiales-20220221-0120.html

Tipo de actividad	Argentina	Brasil	Chile	Colombia	Ecuador	México	Panamá	Perú	Rep. Dominicana	Uruguay	Organización afectada	Descripción de la actividad	Impacto D	Impacto C	Impacto I	Tipo de incidente	Fecha de referencia del incidente	Descripción del incidente	Impacto Cualitativo	Impacto Cuantitativo	Impacto Días impacto	Impacto Costo en dólares	Resolución	Fuente
Energía		X	X	X							Empresas petroleras y mineras	Empresas de extracción y refinado		X	X	Filtración de correos electrónicos y publicación de la información en la plataforma web DDo Secrets.com	3/8/2022	La información proviene de correos electrónicos de firmas de Colombia, Brasil y Chile. De la que se recabó mayor cantidad de datos fue de la empresa minera chilena Quiborax. Revelaron casos de derrames y denuncias de corrupción	Las distintas empresas fueron afectadas de diversas formas, según su materia específica de actividad	Se difundió más de 1TB de información			No informada	https://www.rionegro.com.ar/energia/hackers-filtraron-mas-de-1tb-de-informacion-sobre-petroleras-y-mineras-de-latinoamerica-2427530/
Comercio	X		X	X				X			Cencosud-Supermercados: Easy, Jumbo, Vea y Blainstein	Cadenas de supermercados de venta minorista	X	X		Ransomware-Egregor	17/11/2020	El ataque secuestró las bases de datos con la información de los clientes de las empresas, las que fueron usadas para la extorsión del atacante	Durante la operación ordinaria diaria, las máquinas registradoras imprimieron tickets sin freno con un mensaje en inglés: "Si no pagan, publicaremos toda la información de sus clientes". Preventivamente la empresa cerró sus locales por algunas horas y puso en standby sus sitios web	Inactividad total con el consecuente lucro cesante	1		Se presume que la empresa pagó el rescate pedido	https://www.memo.com.ar/economia/que-hubo-detras-del-ciberataque-a-easy-jumbo-y-vea-en-argentina/
Estado			X	X		X		X			Fuerzas armadas	Defensa militar		X		Fuerza bruta	30/9/2022	Robo de información reservada, principalmente de correo electrónico a través de una brecha de seguridad del servicio Exchange	No informado, debido a la confidencialidad de la información relacionada con la seguridad de cada país	No informado, debido a la confidencialidad de la información relacionada con la seguridad de cada país	No informado debido a la confiden-cialidad de la información relacionada con la seguridad de cada país		No informado, debido a la confidencialidad de la información relacionada con la seguridad de cada país	https://www.bbc.com/mundo/noticias-america-latina-63167331
Logística	X	X	X		X	X	X	X	X	X	Hellmann Worldwide Logistics	Hellmann Worldwide Logistics SE & Co. KG es una empresa alemana de servicios logísticos con sede en Osnabrück, Alemania. Con sucursales en 56 países	X	X		Ransomware-filtración de datos	9/12/2022	Ataque Ransomware y filtración de datos, esta se produjo con anterioridad al secuestro de datos, como primera parte del plan de ataque	Como consecuencia de este ataque ransomware, los clientes de Hellmann están experimentando llamadas y correos electrónicos fraudulentos, según indica la propia compañía en su web. Esta puede ser una de las consecuencias derivadas del ataque. Ya que, si los atacantes no monetizan el incidente a través del cobro del secuestro de datos, lo hacen a través de los datos obtenidos, mediante estafa	Fueron afectados 70.64 GB de datos comprimidos. Estos archivos contienen información como los nombres de clientes, el ID de usuario, correos electrónicos y contraseñas	No especifi-cados, se estima que varias semanas		Se aplicaron soluciones de contingencia de acuerdo con el cada filial y disponibilidad de recursos	https://unaaldia.hispasec.com/2021/12/ataque-ransomware-y-filtracion-de-datos-de-hellmann.html

Tipo de actividad	Argentina	Brasil	Chile	Colombia	Ecuador	México	Panamá	Perú	Rep. Dominicana	Uruguay	Organización afectada	Descripción de la actividad	Impacto D	Impacto C	Impacto I	Tipo de incidente	Fecha de referencia del incidente	Descripción del incidente	Impacto Cualitativo	Impacto Cuantitativo	Días impacto	Costo en dólares	Resolución	Fuente
Tecnología	X	X	X	X	X	X	X	X	X	X	Por las carácterísticas del ataque afectó a cualquier tipo de organizaciones	Por las carácterísticas del ataque afectó a cualquier tipo de actividad		X		Acceso a cuentas y contraseñas de servidores de correo Microsoft	8/1/2021	Filtración de datos en sus servidores in situ de Microsoft Exchange Server	Los atacantes obtuvieron privilegios de administrador en los servidores afectados, acceso a los correos electrónicos y contraseñas de los usuarios y también a los dispositivos conectados a la misma red	250.000 servidores en todo el mundo	90		El 22 de marzo, Microsoft anunció que en el 92% de los servidores in situ de Microsoft Exchange, los efectos del hackeo habían sido corregidos o mitigados	https://blog.mailfence.com/es/analisis-del-hackeo-a-microsoft-exchange-server/
Tecnología	X	X	X	X	X	X	X	X	X	X	Usuarios de Facebook	Utilidades de la aplicación		X	X	Robo y publicación de datos de usuarios de la aplicación	1/3/2021	El ataque dejo expuesta la información personal de millones de usuarios que ha sido publicada en un foro de piratería. Se trata de los correos electrónicos, teléfonos, fechas de nacimiento, biografías, ubicaciones, estado sentimental y biografía	Exposición de información privada	533.000.000 de usuarios afectados	Dadas las caracterís-ticas de los datos expuestos a afectación producida por el ataque perduró en el tiempo, sin poder determinar su duración		No informado	https://www.channelpartner.es/seguridad/noticias/1129859002502/siete-ciberataques-han-marcado-ano-2021.1.html
Finanzas	X	X	X	X	X	X	X	X	X	X	Bancos comerciales/ clientes	Organizaciones cuya actividad económica es la intermediación financiera. Es decir, capta depósitos del público, dirigiendo esos recursos al otorgamiento de créditos, con el objetivo de obtener un beneficio		X	X	Phishing-ingeniería social	19/3/2022	Los clientes de los bancos son víctimas, de ingeniería social como phishing. Estos ciberataques se realizan a través de los correos electrónicos de los usuarios financieros, con el objeto de tratar de capturar o robar información confidencial de los clientes, tales como sus usuarios y contraseñas, números de tarjetas de créditos, entre otras informaciones, para que la víctima voluntariamente revele dichas informaciones mediante técnicas de manipulación y el engaño	Estos crímenes han conllevado, a que los bancos tengan que invertir importantes recursos en realizar campañas de concientización para advertir y educar a los clientes. Asimismo, los bancos deben invertir en programas y herramientas robustas de ciberseguridad para protegerse ante los diferentes ataques cibernéticos	Variable según las víctimas afectadas			La implementada por cada entidad	https://www.diariolibre.com/actualidad/nacional/2022/03/19/victimas-de-fraudes-bancarios-son-por-robo-de-indentidad/1716145
Comercio	X	X	X	X	X	X	X	X	X	X	Pequeñas y medianas empresas y comercios	Actividades varias	X	X	X	Troyano_PSW - ataques de internet-ataques al Protocolo de Escritorio Remoto	Periodo años 2021-2022	De acuerdo con el tipo de ataque en cada caso	De acuerdo con el tipo de ataque en cada caso	De acuerdo con el tipo de ataque en cada caso		155 000	De acuerdo con el tipo de ataque en cada caso	https://latam.kaspersky.com/blog/pymes-latam-enfrentan-creciente-numero-ciberataques/24950

Fuente: Elaboración propia.
Nota: Impacto: D: Disponibilidad, C: Confidencialidad, I: Integridad.

Anexo 2
Información de los CSIRT consultados por país

Listado de CSIRT consultados por información estadística (direcciones obtenidas de la página web de cada uno de ellos:

- cnac@gn.gob.mx: Centro Nacional de Atención Ciudadana México
- contacto@colcert.gov.co: Grupo de Respuesta a Emergencias Cibernéticas de Colombia
- csirt@cedia.org.ec: Equipo de Respuesta a Incidentes de seguridad de Ecuador
- incidentes@cnsd.gob.pe: Centro Nacional de Seguridad Digital - Gobierno del Perú
- soc@csirt.minseg.gob.ar: CSIRT - Ministerio de Seguridad de la Nación Argentina
- ciberseguridad@ba-csirt.gob.ar: Centro de Ciberseguridad Ciudadana de la Ciudad de Buenos Aires
- cais@cais.rnp.br: Centros de Atención a Incidentes de Seguridad
- cctir@citex.eb.mil.br: Centro Integrado de Telemática del Ejército
- certbahia@pop-ba.rnp.br: Grupo de respuesta a incidentes de seguridad de Bahía
- cert@cert.br: CSIRT Brasil
- security@trf3.jus.br: Tribunal Federal 3era Región - Brasil
- ctir@ctir.gov.br: Centro de prevención y Tratamiento de Incidentes Cibernéticos Gubernamentales
- abuse@ctir.aer.mil.br: Centro de Tratamiento de Incidentes de la Fuerza Aérea de Brasil
- abuse@marinha.mil.br: Centro de Tratamiento de Incidentes de la Marina de Brasil
- guardia@cibercrimen.cl: Cibercrimen Santiago
- info@cert.pa: CSIRT del Gobierno de Panamá
- contacto@cncs.gob.do: Centro Nacional de Ciberseguridad de República Dominicana
- cert@cert.uy: Centro Nacional de Respuesta a Incidentes de Seguridad Informática de Uruguay

Anexo 3
Marco Legal y normativo de cada país analizado

Cuadro A1
Argentina

Marco legal 2020	Marco legal 2022
Ley 26.388 de Delito informático. Regulación de los "delitos informáticos" en el Código Penal Argentino Nuevas tendencias criminológicas en el ámbito de los delitos contra la integridad sexual y la problemática de persecución penal	Sin modificación
Ley 25.326 de Protección de Datos Personales. Principios generales relativos a la protección de datos. Derechos de los titulares de datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones. Acción de protección de los datos personales	Sin modificación
Decreto Reglamentario N° 1558/2001. Derechos de los titulares de los datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones	Sin modificación
Ley 25.506 de Firma Digital. Certificados digitales. Certificador licenciado. Titular de un certificado digital. Organización institucional. Autoridad de aplicación. Sistema de auditoría. Comisión Asesora para la Infraestructura de Firma Digital. Responsabilidad. Sanciones. Disposiciones Complementarias	Sin modificación
Decreto Reglamentario N° 2628/2002. Autoridad de Aplicación. Comisión Asesora para la Infraestructura de Firma Digital. Estándares Tecnológicos. Revocación de Certificados Digitales. Certificadores Licenciados. Autoridades de Registro. Disposiciones para la Administración Pública Nacional.	Sin modificación
Ley 26.904 de Grooming. 'Artículo 131: Será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma.'	Sin modificación

Fuente: http://servicios.infoleg.gob.ar/infolegInternet/.

Cuadro A2
Brasil

Marco legal 2020	Marco legal 2022
Marco civil. Establece principios fundamentales para Internet, incluida la libertad de expresión, la neutralidad de la red y la protección de la privacidad	Sin modificación
Ley Nº 13709/2018 - Ley General de Protección de Datos Personales. La finalidad de esta norma es proteger los datos personales, que son definidos como información sobre una persona física identificada o identificable. Mediante esta ley se crea la Autoridad Nacional de Protección de Datos (ANPD)	Sin modificación
Guía de Referencia para la Protección de Infraestructuras Críticas de Información. El Departamento de Seguridad de la Información y Comunicaciones publicó la Guía de Referencia para la Protección de Infraestructuras Críticas de Información y el Libro Verde de Seguridad Cibernética en Brasil	Sin modificación
Ley Nº 12737 sobre delitos cibernéticos. Modifica el Código penal y tipifica los delitos cibernéticos. Según esta norma, las personas que violen las contraseñas u obtengan datos privados y comerciales sin el consentimiento del titular de la cuenta, serán condenadas a penas de entre tres meses y dos años de cárcel, además de abonar una multa	Sin modificación

Fuente: https://ciberseguridad.com/normativa/latinoamerica/brasil/.

Cuadro A3
Chile

Marco legal 2020	Marco legal 2022
Ley N°19.223 - Tipifica figuras paneles a la informática	Ley 21459 - Deroga la ley Nº 19233 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest - Delitos Informáticos, Sistemas Informáticos, Integridad Informática, Interceptación Ilícita, Falsificación Informática, Receptación, Fraude Informático, Circunstancias Atenuantes, Circunstancias Agravantes, Datos Informáticos
Ley Nº 19.799 - 25032002. Sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma	Sin modificación
Decreto Nº181 - 09072002. Ministerio de Economía; Fomento y Reconstrucción; Subsecretaría de Economía; Fomento y Reconstrucción, que aprueba reglamento de la Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma	Sin modificación
Decreto Nº83 - 03062004. Ministerio Secretaría General de la Presidencia. Aprueba norma técnica para los órganos de la administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos	Sin modificación
Ley Nº 20.217 - 05102007. Ministerio de Economía, Fomento y Reconstrucción, Subsecretaría de Economía, Fomento y Reconstrucción. Modifica el Código de Procedimiento y la Ley nº 19.799 sobre documento electrónico, firma electrónica y servicios de certificación de dicha firma	Sin modificación
Decreto Nº154 – 11112011. que modifica Decreto nº 181, de 2002, que aprueba Reglamento de la Ley nº 19.799 sobre Documentos Electrónicos, Firma Electrónica y la Certificación de dicha Firma, del Ministerio de Economía, Fomento y Turismo;	Sin modificación
Decreto Nº24 – 22022019. Ministerio de Economía, Fomento y Turismo; Subsecretaria de Economía y Empresas de menor tamaño, que aprueba Norma Técnica para la prestación del Servicio de Certificación de Firma Electrónica Avanzada	Sin modificación

Fuente: https://www.informatica-juridica.com/legislacion/chile/.

Cuadro A4
Colombia

Marco legal 2020	Marco legal 2022
Ley Nº 2015-31012020. Creación de la Historia Clínica Electrónica Interoperable (HCEI) y se dictan otras disposiciones	Sin modificación
Proyecto de Ley 300 de 2020-11032020 (modificatoria anteriores). Disposiciones generales para el fortalecimiento de la protección de datos personales, con relación al reconocimiento de las garantías de los derechos digitales, y se dictan otras disposiciones.	Sin modificación
Resolución Nº 12192 - 01042020 / Resolución Nº 19587- 28042020 / Resoluciones Nº 24913 Nº 24923 Nº 24924 Nº 25171 Nº 25173 Nº 25174 Nº 25176 Nº 25177-29052020. Protección de Datos Personales. Dictadas ante casos específicos planteados	Sin modificación
Resoluciones Nº 30412 Nº 30489 – 23062020 Protección de Datos Personales. Dictadas ante casos específicos planteados	Sin modificación
Resoluciones Nº 33217 Nº 33222 Nº 33267. Nº 34638 Nº 34913 Nº 35093 Nº 38281 – 30062020. Protección de Datos Personales. Dictadas ante casos específicos planteados	Sin modificación
Resoluciones Nº 43198 Nº 43704 Nº 43761 Nº 43861 Nº 43862 - 30072020 - Protección de Datos Personales. Dictadas ante casos específicos planteados	Sin modificación
Decreto 1154 - 20082020 (modificatorio) – Modifica el Capítulo 53 del Título 2 de la Parte 2 del Libro 2 del Decreto 1074 de 2015, Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, referente a la circulación de la factura electrónica de venta como título valor y se dictan otras disposiciones	Sin modificación

Marco legal 2020	Marco legal 2022
Ley 2052 - 25082020 - Se establecen disposiciones transversales a la rama ejecutiva del nivel nacional y territorial y a los particulares que cumplan funciones públicas y/o administrativas, en relación con la racionalización de trámites y se dictan otras disposiciones	Sin modificación
Resoluciones Nº 50091 Nº 52391 Nº 52394 – 25082020 Protección de Datos Personales. Dictadas ante casos específicos planteados	Sin modificación
Decreto 045 - 15012021 (derogación) - Se derogan el Decreto 704 de 2018 y el artículo 1.1.2.3. del Decreto 1078 de 2015, Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones	Sin modificación
Directiva Presidencial Nº 03 - 15032021 - Lineamientos para el uso de servicios en la nube, Inteligencia Artificial, Seguridad Digital y Gestión de Datos	Sin modificación
	Decreto 088 - 24012022 (reglamentario). Se adiciona el Título 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los artículos 3, 5 y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea
	Decreto 255 - 23022022, por el cual se adiciona la Sección 7 al Capítulo 25 de la Parte 2 del Libro 2 del Decreto 1074 de 2015 - Normas corporativas vinculantes para la certificación de buenas prácticas en protección de datos personales y su transferencia a terceros países
	Decreto Nº 338 - 08032022 - Establece los lineamientos generales para fortalecer la gobernanza de la seguridad digital y crea el modelo y las instancias de gobernanza de seguridad digital entre otras disposiciones
	Decreto nº 767 - 16052022 - Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

Fuente: https://www.informatica-juridica.com/legislacion/colombia/.

Cuadro A5
Ecuador

Marco legal 2020	Marco legal 2022
Acuerdo Ministerial Nº 035-2020 del Ministro de Telecomunicaciones y de la Sociedad de la Información. Guía de Datos Abiertos de aplicación en la Administración Pública Central. (Suplemento nº 361 del Registro Oficial - 15012021)	Sin modificación
Acuerdo Ministerial Nº 076-2020-MDT - 12032020. Directrices para la aplicación de Teletrabajo emergente durante la declaración de emergencia sanitaria	Sin modificación
Acuerdo Ministerial nº 265-2020-MDT - 13122020 - Reforma el Acuerdo Ministerial nº 076-2020-MDT de 12 de marzo de 2020	Sin modificación
Guía de Datos Abiertos - 15012021 - Implementación de las directrices de la política, y cuyo objetivo es proporcionar criterios técnicos y metodológicos para planificar, abrir, publicar y promover la utilización de los datos abiertos gubernamentales	Sin modificación
Proyecto de Ley Orgánica - 07052021 - Reformatoria del Código Orgánico Integral Penal para prevenir y combatir la violencia sexual digital y fortalecer la lucha contra los delitos informáticos	Sin modificación
Acuerdo Ministerial nº 006-2021 - 17052021 - Del Ministro de Telecomunicaciones y de la Sociedad de la Información, que publica la Política de Ciberseguridad	Sin modificación
Ley Orgánica de Protección de Datos - 21052021 - Registro Oficial	Sin modificación

Marco legal 2020	Marco legal 2022
Ley Orgánica reformatoria del Código Orgánico - 31082021 - Prevenir y combatir la violencia sexual digital y fortalecer la lucha contra los delitos informáticos	Sin modificación
	Oficio nº MINTEL-MINTEL-2022-0975-O - 09082022 - Socialización de la aprobación de la Estrategia Nacional de Ciberseguridad de Ecuador

Fuente: https://www.informatica-juridica.com/legislacion/ecuador/.

Cuadro A6
México

Marco legal 2020	Marco legal 2022
Código Penal Federal - Última Reforma DOF 12-11-2021 - Regulación sobre delitos financieros, seguridad de la información y el uso de tecnología en otros delitos, como terrorismo, secuestro y narcotráfico	Sin modificación
Ley Federal de Telecomunicaciones y Radiodifusión - 20052021 - Ley federal de telecomunicaciones y radiodifusión, y la ley del sistema público de radiodifusión; y se reforman, adicionan y derogan diversas disposiciones de la materia	Sin modificación
Ley Federal de Protección de Datos Personales en poder de Particulares - 05072010 - Sus reglamentos, recomendaciones, directrices y reglamentos similares sobre protección de datos	Sin modificación
Ley Federal de Transparencia y Acceso a la Información Pública - 11062002 - Reconoce y regula el derecho individual al acceso a la información de las instituciones y organismos del Estado	Sin modificación
Normas Generales - Norma Oficial Mexicana (NMX) - 14042015 - Normas oficiales obligatorias para todo tipo de organizaciones	Sin modificación
Ley de la Policía Federal - 01062009 - Se reforman, adicionan y derogan diversas disposiciones de la Ley Federal de Telecomunicaciones	Sin modificación
Marco Normativo	
NMX-I-27001-NYCE-2015 - Tecnologías de la Información-Técnicas de Seguridad-Sistemas de Gestión de Seguridad de la Información -Requisitos, que reproduce las disposiciones establecidas en la ISO / IEC 27001: 2013 Tecnología de la información-Técnicas de seguridad-Sistemas de gestión de seguridad de la información-Requisitos	Sin modificación
NMX-I-27001-NYCE-2015 - Tecnologías de la Información-Técnicas de Seguridad-Código de Buenas Prácticas para el Control de la Seguridad de la información, que reproduce las disposiciones establecidas en la ISO / IEC 27002: 2013 Information Technology-Security Técnicas-Código de prácticas para los controles de seguridad de la información.	Sin modificación

Fuente: https://revistaseguridad360.com/destacados/ley-de-ciberseguridad-en-mexico/#Legislacion. https://ciberseguridad.com/normativa /latinoamerica/mexico/#Legislacion.

Cuadro A7
Panamá

Marco legal 2020	Marco legal 2022
Ley 43 - 31072001 - Define y regula los documentos electrónicos y firmas y certificaciones autorizadas del comercio electrónico.	Sin modificación
Código Penal - 18052007 - Delitos contra la Seguridad Jurídica de los Medios Electrónicos	Sin modificación
Ley 51 - 18092009 - Normas para la Conservación, la Protección y el Suministro de Datos de Usuarios de los Servicios de Telecomunicaciones	Sin modificación

Fuente: https://www.informatica-juridica.com/legislacion/panama/.

Cuadro A8
Perú

Marco legal 2020	Marco legal 2022
Ley 27309 - 17072000 - Incorporación los delitos informáticos al Código Penal	Sin modificación
Resolución Jefatural 347-2001-INEI - 07112001 - Aprueban Directiva "Normas y procedimientos técnicos para garantizar la seguridad de la información publicadas por las entidades de la administración pública"	Sin modificación
Resolución Ministerial 0391-2009-AG - 19052009 - Aprobación e institucionalización el documento "Política de Seguridad de la Información"	Sin modificación
Ley 30096 - 22102013 - Ley de delitos informáticos	Sin modificación
Decreto Supremo 012-2013-IN - 28072013 - Se aprueba política nacional del estado peruano en seguridad ciudadana	Sin modificación
Resolución Ministerial 166-2017-PCM - 21062017 - Modificación del artículo 5 de la R.M. 004-2016-PCM referente al comité de gestión de Seguridad de la Información	Sin modificación
Decreto Supremo 050-2018-PCM - Se aprueba la definición de seguridad digital en el ámbito nacional (1505/2018)	Sin modificación
Ley 30999 - 27082019 - Ley de ciberdefensa	Sin modificación
Marco Normativo	
NTP-ISO/IEC 17799:2004- 2007 EDI Tecnología de la información - 23072004 - Código de buenas prácticas para la gestión de la seguridad de la información. 1ª edición." en entidades del sistema	Sin modificación
NTP ISO/IEC 27001:2008 EDI tecnología de la información - 25052012 - Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos en todas las entidades integrantes del sistema nacional de informática	Sin modificación
ISO NTP/IEC 27001:2014 Tecnología de la Información - 08012016 - Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos 2a. Edición", en todas las entidades integrantes del sistema nacional de informática	Sin modificación
NTP ISO IEC 27001:2008 EDI tecnología de información - Técnicas de seguridad. Sistemas de gestión de seguridad de la información	Sin modificación

Fuente: https://www.congreso.gob.pe/carpetatematica/2018/carpeta_122/normas_nacionales/.

Cuadro A9
República Dominicana

Marco legal 2020	Marco legal 2022
Decreto nº 709-07 - 26122007 - Se instruye a toda la Administración Pública a cumplir con las normas y los estándares tecnológicos	Sin modificación
Ley nº 53/2007 - 23042007 - Protección integral de los sistemas que utilicen tecnologías de información y comunicación y su contenido	Sin modificación
Ley Orgánica 172-13. Protección de Datos de Carácter Personal de la República Dominicana -26112013- Protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes	Sin modificación

Fuente: https://www.informatica-juridica.com/legislacion/republica-dominicana/.

Cuadro A10
Uruguay

Marco legal 2020	Marco legal 2022
Ley Nº 18.381 - 17102008 - Derecho de Acceso a la Información Pública	Sin modificación
Decreto N° 664/008 - 22122008 - Creación el Registro de Bases de Datos Personales	Sin modificación
Ley Nº 18.600 - 21092009 - Documento electrónico y la firma electrónica	Sin modificación
Decreto 437/2009 - 28092009 - Protección de datos personales. Bases de datos	Sin modificación
Decreto 451/2009 - 28092009 - Reglamentación del Centro Nacional de Respuesta a Incidentes de Seguridad Informática	Sin modificación
Decreto Nº 452/2009 - 28092009 - Política de seguridad de la información para Organismos de la Administración Pública	Sin modificación
Decreto nº 64/020 - 17022020 - Reglamentación de los artículos 37 a 40 de la Ley 19.670 y artículo 12 de la Ley 18.331, referente a Protección de Datos Personales	Sin modificación

Fuente: https://www.informatica-juridica.com/legislacion/uruguay/.

En el marco del acelerado proceso de digitalización de los últimos años, se hace necesaria una mayor atención de los países de América Latina y el Caribe al aumento de los incidentes en materia de seguridad cibernética que afectan a sus principales infraestructuras críticas. Para ello es necesario priorizar el tema tanto en las agendas digitales como en las políticas públicas nacionales. En el último año, se han producido importantes avances en los marcos normativos, así como en la institucionalidad encargada de llevar adelante las estrategias de ciberseguridad de los países de la región. Sin embargo, aún falta mucho por hacer. El objetivo de este documento es avanzar en la identificación de las políticas dirigidas a atender a los incidentes de ciberseguridad ocurridos entre 2020 y 2022 en diez países seleccionados de América Latina. Además de la información obtenida por los equipos de respuesta a incidentes de ciberseguridad, se incluyen informes publicados por instituciones especializadas en estos temas, que complementan la información proporcionada en este trabajo.

CEPAL

Comisión Económica para América Latina y el Caribe (CEPAL)
Economic Commission for Latin America and the Caribbean (ECLAC)
www.cepal.org

LC/TS.2023/93