ISSN 1680-8754

SERIE

DESARROLLO PRODUCTIVO 228

Estado de la ciberseguridad en la logística de América Latina y el Caribe

Rodrigo Mariano Díaz

NACIONES UNIDAS

CEPAL

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

NACIONES UNIDAS

CEPAL

www.cepal.org/es/publications

facebook.com/publicacionesdelacepal

www.cepal.org/apps

SERIE

DESARROLLO PRODUCTIVO | 228

Estado de la ciberseguridad en la logística de América Latina y el Caribe

Rodrigo Mariano Díaz

NACIONES UNIDAS

CEPAL

Este documento fue preparado por Rodrigo Mariano Díaz, Consultor de la División de Desarrollo Productivo y Empresarial de la Comisión Económica para América Latina y el Caribe (CEPAL), y fue coordinado por Georgina Núñez, Oficial de Asuntos Económicos de la Unidad de Inversiones y Estrategias Empresariales de la misma División, y por Ricardo Sánchez, Jefe de la Unidad de Servicios de Infraestructura de la División de Comercio Internacional e Integración de la CEPAL.

Los coordinadores y el autor agradecen a Felipe Harboe, en su calidad de académico de Protección de Datos del Diplomado en Compliance de la Pontificia Universidad Católica de Chile, por sus comentarios en la revisión final de este documento.

Las opiniones expresadas en este documento, que no ha sido sometido a revisión editorial, son de exclusiva responsabilidad del autor y pueden no coincidir con las de la Organización.

Publicación de las Naciones Unidas
ISSN: 1680-8754 (versión electrónica)
ISSN: 1020-5179 (versión impresa)
LC/TS.2021/108
Distribución: L
Copyright © Naciones Unidas, 2021
Todos los derechos reservados
Impreso en Naciones Unidas, Santiago
S.21-00485

Esta publicación debe citarse como: R. Díaz, "Estado de la ciberseguridad en la logística de América Latina y el Caribe", *serie Desarrollo Productivo*, N° 228 (LC/TS.2021/108), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2021.

La autorización para reproducir total o parcialmente esta obra debe solicitarse a la Comisión Económica para América Latina y el Caribe (CEPAL), División de Documentos y Publicaciones publicaciones.cepal@un.org. Los Estados Miembros de las Naciones Unidas y sus instituciones gubernamentales pueden reproducir esta obra sin autorización previa. Solo se les solicita que mencionen la fuente e informen a la CEPAL de tal reproducción.

Índice

Gráficos

Resumen

Los cambios vertiginosos, producidos por las tecnologías pertenecientes a la cuarta revolución industrial en la transición hacia la logística 4.0 impactarán a los países, las empresas, las industrias, y la sociedad en su conjunto.

La pandemia por el COVID-19 ha afectado la producción, las exportaciones e importaciones de América Latina y el Caribe. Al mismo tiempo que se ha transformado en catalizador de la digitalización acelerando el proceso de transición y lograr mantener las operaciones durante el aislamiento, y recuperarlas paulatinamente, reduciendo la interacción entre las personas. Para lograr mantener la base operativa, las organizaciones han abierto filiales virtuales en los hogares para continuar el trabajo en modalidad *home office.*

En este contexto, las amenazas a la ciberseguridad preexistentes y empoderadas son ya una realidad. Desde el inicio de la pandemia, además de los problemas operativos de los centros logísticos, los ciberataques han aumentado y las actividades logísticas siguen estando entre los sectores económicos más afectados. La evidencia muestra un incremento de los ciberataques en el último año, a pesar de no contar con toda la información sobre la infraestructura crítica, y las cadenas logísticas.

Introducción

El objetivo principal de este estudio es realizar un diagnóstico de los acontecimientos relacionados con la ciberseguridad, ocurridos en los últimos 5 años y especialmente durante el brote de COVID-19 en América Latina y el Caribe, para analizar las tendencias técnicas en la región, y así poder trazar un plan de acción que acompañe la recuperación del sector logístico, fuertemente vinculado a las tecnologías disruptivas pertenecientes a la cuarta revolución industrial.

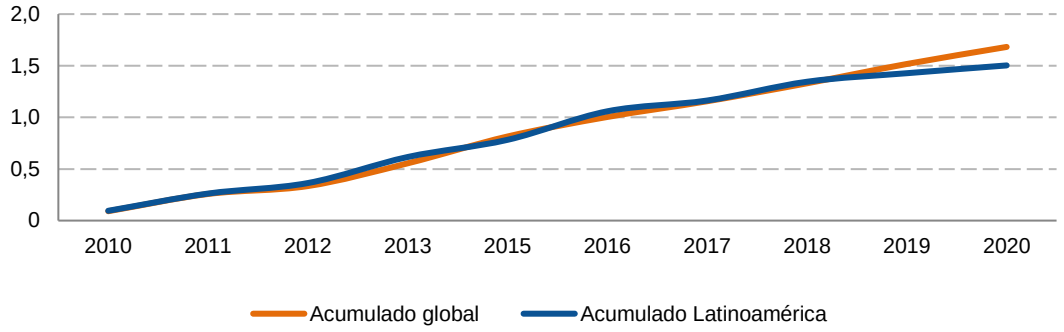
Para lograr este objetivo, se ha recolectado información por tres vías. Por un lado, se realizó una investigación con información secundaria recopilada de las organizaciones públicas y privadas relacionadas con la prevención, detección y corrección de brechas de ciberseguridad en LAC. Además, se realizó un inventario de los incidentes de ciberseguridad conocidos en la región en los últimos cinco años que afectaron infraestructura propia de cadenas logísticas u organizaciones que hayan impactado en esta. Finalmente, se realizó una encuesta a 46 directores y gerentes de organizaciones relacionadas con la logística regional sobre los sucesos relacionados con la ciberseguridad durante el último año, y sus preocupaciones y estrategias para los siguientes doce meses. Para ello, se distribuyó un cuestionario con 23 preguntas dirigidas a relevar las incidencias del último año y su impacto correspondiente, la preparación general de las organizaciones de las que forman parte y las preocupaciones para los próximos 12 meses. El resultado se ha evaluado de manera general para toda la región de América Latina y el Caribe en el capítulo IV de este documento. Al mismo tiempo se ha individualizado y anexado las variaciones en las respuestas según los países donde operan las organizaciones que participaron del cuestionario. La logística 4.0 durante la pandemia de COVID-19 y la ciberseguridad.

Las tecnologías clave de la 4ta revolución industrial como el Internet de las cosas (Iot), la automatización, el blockchain, el big data y el cloud computing, están conduciendo la logística a nivel global, hacia la logística 4.0, lo que demanda la solución de temas como la alfabetización digital, el costo y la velocidad de acceso a internet, así como la ciberseguridad. En un estudio desarrollado por Barleta, Pérez, y Sánchez, (2019) exploraron el uso y explotación de los datos como diferenciador,

entre las empresas que toman beneficio de la transformación digital y aquellas que, por no hacerlo, estarán en serios riesgos de subsistencia, dejando una interrogante del momento basada en que dicha transformación sería clave para la nueva manera de operar dentro de la logística.

El COVID-19 ha sido un importante catalizador del proceso de transformación digital, acelerando los tiempos de adopción y aumentando las escalas, respondiendo a la necesidad de mantener a las organizaciones en operación durante el aislamiento ocurrido a partir del mes de marzo 2020 en la región, en algunos casos, y en otros, ha permitido continuar operando bajo protocolos estrictos, con el fin de reducir los contagios. Pero además de los cambios que se han experimentado durante estos meses, se está observando un cambio estratégico en las organizaciones respecto a la tecnología. Según IDG, organización destinada a fortalecer el correcto uso de la tecnología, las 3 prioridades en las organizaciones para los próximos 12 meses son liderar la transformación digital, mejorar la experiencia de trabajo remoto de los colaboradores de sus organizaciones y mejorar la ciberseguridad para aumentar la resiliencia de sus organizaciones (IDG, 2020). En simultáneo con la aceleración de la transformación digital y la depresión económica global, la industria del cibercrimen ha aumentado en complejidad, a través del uso de herramientas de *machine learning* y de inteligencia artificial, y en volumen, a través del mercado de *malware* como servicio (Maas) ofrecido en la *deep web*. Al mismo tiempo, la pandemia ha llevado a un incremento anual del 1,5% del tráfico total en internet, y ha cambiado el hábito de uso, ya que, para el mismo período de tiempo, las transacciones se incrementaron en un 26,7% (Clement, 2020). Al mismo tiempo, en la región ha aumentado en un 150% la cantidad de usuarios conectados desde el año 2010 como se observa en el gráfico 1, manteniendo la misma pendiente creciente prácticamente igual que en el resto del planeta (Clement, 2020).

Gráfico 1
Crecimiento de usuarios conecctados a Internet
(En porcentajes)



Fuente: Elaboración propia con datos de Internet World Stats, www.internetworldstats.com.

Tanto el crecimiento de ofertas en el mercado de la ciberdelincuencia, como el aumento de uso de la tecnología en cantidad de usuarios conectados y en transacciones, en parte motivados por la continuación de las actividades humanas, dan por resultado un aumento interanual para el mes de octubre de 2020 de 67% de ataques de *ransomware*, 71% de *malware* a través de páginas web seguras y de 510% para ataques a dispositivos de internet de las cosas (Sonicwall, 2020).

Este escenario emergente encontró a los distintos países de la región con diferentes grados de maduración en ciberdefensa, registrándose este efecto tanto en el ámbito privado como público. Es de destacar que el fenómeno de la cibercriminalidad impone en las comunidades un proceso complejo que nace con la toma de conciencia ante la evidencia contundente del alcance y poder de daño de los

ciberataques. Para dar tratamiento orgánico a esta problemática, en el año 2018 la Unión Internacional de Telecomunicaciones (UIT), división de Naciones Unidas, en conjunto con otras organizaciones, redactaron la "Guía para la elaboración de una estrategia nacional de ciberseguridad" donde se define el rol del estado en la elaboración de una *Estrategia Nacional de Ciberseguridad* (NCS por sus siglas en inglés) (UIT, 2018). En la NCS se asignan prioridades y recursos nacionales, lo cual resulta oportuno para desarrollar la discusión y definición de la legislación adecuada para combatir y penalizar estos delitos, donde el cuerpo legal en muchos casos es frágil o ausente.

El Convenio de Budapest que se firmó el 23 de noviembre de 2001 y entró en vigor el 1° de julio de 2004, en la ciudad de Budapest, República de Hungría, es el primer tratado internacional creado con el objetivo de **proteger a la sociedad frente a los delitos informáticos y los delitos en Internet**, mediante la elaboración de leyes adecuadas, la mejora de las técnicas de investigación y el aumento de la cooperación internacional y ha sido la referencia, originalmente de la Unión Europea, extendiéndose luego al resto del planeta, para la creación de las leyes nacionales de protección contra el ciberdelito. En la actualidad, el Convenio ha sido ratificado por más de 50 naciones de todo el mundo y en particular en LAC forman parte de este convenio, Argentina, Chile, Colombia, Costa Rica, Panamá, Paraguay, Perú y República Dominicana .

Abordadas las etapas estratégicas y legales, los países se encontrarían en el plano "posible" de incorporar el marco regulatorio que contribuya a mitigar la incidencia de esta modalidad criminal en la institucionalidad, la economía y la vida de los individuos de cada país. La regulación o normativa local aplicada a ciberseguridad, se transforma entonces, en un elemento esencial para lograr gestionar la incidencia, a la vez que el soporte de esta es la capacidad operativa de los organismos de aplicación, entendiéndose a esta última, como la capacidad de reducir al mínimo posible el tiempo que transcurre entre la detección del incidente y el inicio de la gestión sobre el mismo.

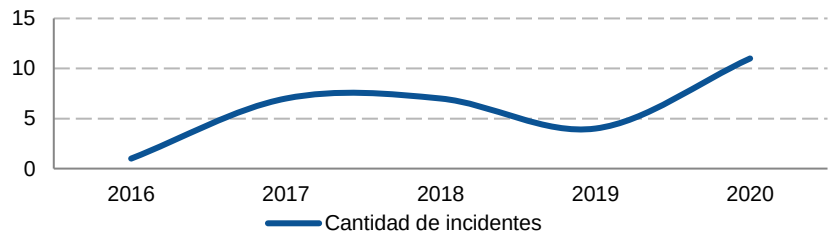
Alineados con las NCS, los Equipos de Respuesta a Incidentes de Seguridad o CSIRT (sigla de *Cyber Security Incident Response Team*), que pueden definirse en los ámbitos académicos, gubernamentales, militares o privados, son los centros operativos claves con los que puede contar un estado para minimizar y controlar los daños ante un ciberataque. Al mismo tiempo asesoran, responden y recuperan la normalidad en las operaciones, así como previenen la ocurrencia de futuros incidentes (NIST, 2012).

I. Incidentes de ciberseguridad ocurridos en las cadenas logísticas

De acuerdo con los resultados de las estadísticas mencionadas en el apartado anterior, y continuando la línea de trabajo comenzada por CEPAL y publicada en noviembre de 2020 a través del boletín FAL N° 382, se ha realizado un inventario de incidentes de ciberseguridad denunciados y expuestos públicamente, que se presentan a continuación.

Según las investigaciones realizadas sobre organizaciones relacionadas con la cadena logística o cuya actividad pueda afectar directamente a esta, en los últimos 5 años se registran 30 incidentes de conocimiento público, de los cuales 11 ocurrieron durante 2020. Como puede observarse en el gráfico 2, esta cifra no solo supera en un 57% los años 2017 y 2018 en los cuales los ransomware WannaCry y NotPetya se propagaron fuertemente afectando a todo tipo de industria, particularmente en logística y transporte dejaron casos conocidos como el de la firma Maersk con una pérdida de US$ 300 millones, sino que representa un crecimiento del 175% con relación al 2019. Es decir que en 2020 se registraron incidentes que casi triplicaron la cantidad del año anterior.

Gráfico 2
Incidentes registrados en logística



Fuente: Investigación CEPAL.

Cuadro 1
Registros de incidentes por actividad en América Latina por país (2020)

Fecha del incidente	Argentina	Brasil	Chile	Colombia	Ecuador	México	Panamá	Perú	República Dominicana	Uruguay	Organización	Nombre del Puerto	Actividad Principal	Pilar Afectado D: Disponibilidad C: Confidencialidad I: Integridad			Tipo de incidente	Descripción del Incidente	Impacto		N°
														D	C	I			Cualitativo	Cuantitativo (En dólares)	
20/5/2016					X						Banco del Austro		General de la actividad			X	Vulnerabilidad de día cero en la red SWIFT	Transferencias monetarias por la red SWIFT. Fallas en los controles por parte de la empresa operadora de la red.	Debilidad del banco por no mantener actualizada la red en cuestión	9 000 000	(1)
13/5/2017						X					Aeropuertos y servicios auxiliares		Administración y operación de aeropuertos	X			Ransomware Wanna Decryptor	Acceso a servidores bloqueado	No se cuenta con información		(2)
13/5/2017		X									Petrobras		Productor, distribuidor y comercializador de petroleo y sus derivados.	X			Ransomware WannaCry	Acceso a servidores bloqueado	Varias refinerías		(3)
31/5/2017	X										Nidera - Puerto San Martín	Puerto San Martin	Producción de aceite Embarque de aceite	X			Ransomware	Aplicaciones comerciales y de logística bloqueadas	Se paralizó la descarga de camiones, la producción y embarque de aceite, la compra de mercadería y pagos de operaciones		(4)
26/6/2017						X					APM Terminals México	Lázaro Cárdenas	Contenedores	X			Virus GoldenEyes	Acceso a servidores bloqueado	La operación debe realizarse en forma manual, pudiendo solo realizar la descarga de los contenedores	900 000	(5)
27/6/2017	X	X	X	X		X	X	X		X	Maersk		Contenedores	X			Ramsomware Petya	Acceso a servidores bloqueado	Afectó a todas las unidades de negocio en Maersk–Envío de contendores, operaciones del puerto y remolcadores, producción de gas y petróleo, servicios de perforación y buques petroleros	300 000 000	(6)
27/6/2017								X			APM Terminals Callao	Callao	Contenedores Carga general Pasajeros	X			Ramsomware Petya	Acceso a servidores bloqueado	Afectó a todas las unidades de negocio. Envío de contendores, operaciones del puerto y remolcadores.		(7)
29/6/2017	X										Cofco Intl.	Timbues	Carga de graneles	X			Ransomware	Aplicaciones comerciales y de logística bloqueadas	Se paralizó la descarga de camiones, la compra de mercadería y pagos de operaciones		(8)
28/12/2017		X									Clarkson Plc		Servicios General		X		Robo de contraseña	Acceso a servidores bloqueado	2% de caída en las acciones de la firma		(9)

Fecha del incidente	Argentina	Brasil	Chile	Colombia	Ecuador	México	Panamá	Perú	República Dominicana	Uruguay	Organización	Nombre del Puerto	Actividad Principal	Pilar Afectado D: Disponibilidad C: Confidencialidad I: Integridad			Tipo de incidente	Descipción del Incidente	Impacto		N°
														D	C	I			Cualitativo	Cuantitativo (En dólares)	
24/5/2018			X								Banco Estado (1)		General de la actividad	X			Malware #killdisk / #killMBR	Imposibilidad de re-inicio de los equipos	9000 pc y 500 servidores (de variadas plataformas)		(10)
24/5/2018			X								Banco Estado (2)		General de la actividad			X	Vulnerabilidad de día cero en la red SWIFT	Mientras la institución se encontraba dedicada a la resolución del malware que afectaba a los equipos, los atacantes realizaban transferencias monetarias por la red SWIFT	Debilidad del banco por no mantener actualizada la red en cuestión	10 000 000	(11)
17/7/2018	X	X	X	X		X	X	X		X	TNT Express		Logistica. Entrega de mensajeria y encomiendas	X			Ransomware Petya	Acceso a servidores bloqueado	Paralización inicial y posteriores retrasos en el servicio de entrega que impactó en la facturación	300.000.000	(12)
24/7/2018	X	X	X				X	X		X	Cosco Shipping		Contenedores	X			Malware/Ransomware	Servidores de correo electrónico bloqueados	Segun declara la empresa, este ataque no impactó en la continuidad del negocio		(13)
17/8/2018								X			Asociación de Bancos del Perú (Asbanc)		General de la actividad	X			Ransomware SamSam	Acceso a servidores bloqueado	El ataque fue detectado en proceso a varias instituciones, por lo que no se conoció el impacto, tanto en general como espcífico de cada institución		(14)
24/1/2019	X										Cooperativa 16 de Octubre		Empresa que presta servicios de energía eléctrica, agua potable y saneamiento en las localidades de Esquel y Trevelin (Chubut)	X			Ransomware WannaCry	Bloquedo el acceso a las aplicaciones de facturación, gestión de reclamos de los clientes y liquidación de sueldos de los empleados	Los servicios que brinda la empresa no se ven afectados, pero la empresa pierde el control sobre los mismos con alto perjuicio económico	3 000	(15)
2/7/2019			X								T.P.A. S.A.	Terminal Portuaria Arica	General	X			Malware	Sitios web, correos electrónicos, facturación y todos los servicios vía Internet deben inactivarse por detección de virus.	Debe migrarse a operación manual		(16)
2/7/2019			X								Puerto Angamos S.A.	Angamos	Minerales Contenedores	X			Malware	Sitios web, correos electrónicos, facturación y todos los servicios vía Internet deben inactivarse por detección de virus.	Debe migrarse a operación manual		(17)

Fecha del incidente	Argentina	Brasil	Chile	Colombia	Ecuador	México	Panamá	Perú	República Dominicana	Uruguay	Organización	Nombre del Puerto	Actividad Principal	Pilar Afectado D: Disponibilidad C: Confidencialidad I: Integridad			Tipo de incidente	Descipción del Incidente	Impacto		N°
														D	C	I			Cualitativo	Cuantitativo (En dólares)	
2/7/2019			X								Terminal Pacifico Sur Valparaiso S.A.	Vaparaiso	Contenedores Carga general Pasajeros	X			Malware	Sitios web, correos electrónicos, facturación y todos los servicios vía Internet deben inactivarse por detección de virus.	Debe migrarse a operación manual		(18)
2/7/2019			X								Ultramar / Ultraport		Agencia marítima	X			Malware	Sitios web, correos electrónicos, facturación y todos los servicios vía Internet deben inactivarse por detección de virus.	Debe migrarse a operación manual		(19)
10/11/2019						X					Pemex		Productor, distribuidor y comercializador de petroleo y sus derivados.	X			Ransomware Sodinokibi	Acceso bloqueado al 5% del equipamiento	No fueron afectados los procesos centrales (extracción, logística, refinación y comercialización)	50 000 000	(20)
11/3/2020		X									Cosan Limited		Productor, distribuidor y comercializador de combustibles	X			Ransomware Nefilim	Acceso a servidores bloqueado	Todos sus procesos afectados		(21)
30/3/2020									X		Autoridad Portuaria de la República Dominicana		Función pública específica de su actividad			X	Strong	Alteración de la página web de la Autoridad Portuaria de República Dominicana, inyectando sobre ella contenido reivindicativo genérico y un fichero 404javascript.js con su alias.	Ciberdebilidad que afecta la reputación de la organización		(22)
10/4/2020	X										Mediterranean Shipping Company Argentina	Puerto de Buenos Aires	Contenedores	X			Malware	Caida de plataformas WEB residentes en servidores centrales (Ginebra)	Debido a la caída de los servidores centrales, la filial argentina entra en contingencia por vias alternativas.		(23)
8/6/2020		X									LIGHT ENERGIA S.A.		Distribuidor de Energía Eléctrica	X			Ransomware Sodinokibi	Acceso a servidores bloqueado	No informado	14 000 000	(24)
30/6/2020		X									CPFL Energia		Generación y distribución de energía eléctrica		X		Ransomware Maze	Acceso a servidores bloqueado	Robo de información sensible (estimado desde mayo a junio del año 2020)		(25)

Fecha del incidente	Argentina	Brasil	Chile	Colombia	Ecuador	México	Panamá	Perú	República Dominicana	Uruguay	Organización	Nombre del Puerto	Actividad Principal	Pilar Afectado D: Disponibilidad C: Confidencialidad I: Integridad			Tipo de incidente	Descipción del Incidente	Impacto		N°
														D	C	I			Cualitativo	Cuantitativo (En dólares)	
30/7/2020	X	X	X	X	X	X	X	X	X	X	Garmin		Fabricación y soporte de GPS GPS para el ámbito civil, principalmente para tránsito terrestre, aunque también naval y aéreo	X			Ransomware WastedLocker	Acceso a servidores bloqueado	Durante 5 dias quedaron sin soporte de ubicación geografica todos sus usuarios		(26)
3/8/2020						X					CIBanco		General de la actividad		X		Ransomware Sodinokibi	Acceso a servidores bloqueado	No informado		(27)
28/9/2020	X	X	X	X	X	X	X	X	X	X	CMA CGM		Contenedores	X	X		Malware	CMA CGM se refirió a la supuesta filtración de datos tras un ataque cibernético que afectó a sus servidores periféricos el lunes 28 de septiembre, lo que impidió que clientes y usuarios ingresaran al sitio web de la naviera y hacer uso de sus aplicaciones informáticas.	12 días sitio de e-commerce Offline		(28)
28/9/2020	X	X	X	X	X	X	X	X	X	X	CMA CGM		Transporte de contenedores	X	X		Ransomware Ragnar Locker	Servidores comercio electrónico	Tan pronto como se detectó la brecha de seguridad, se interrumpió el acceso externo a las aplicaciones para evitar que el malware se propagara.		(29)
4/10/2020		X									Braskem		Petroquímica. Resinas y otros derivados	X			Ransomware Sodinokibi	Acceso a servidores bloqueado	Retrasos en la entrega de productos que impactó en 45% la facturación durante la afectación		(30)

Fuente: Elaboración propia basado en información publicada en sitios web.

Nota: (1) 20/5/2016, Banco Ecuatoriano Cae Víctima de los Cibercriminales. https://hipertextual.com/. Recuperado en nov-20. Véase en línea: https://hipertextual.com/2016/05/hackeo-banco-del-austro.

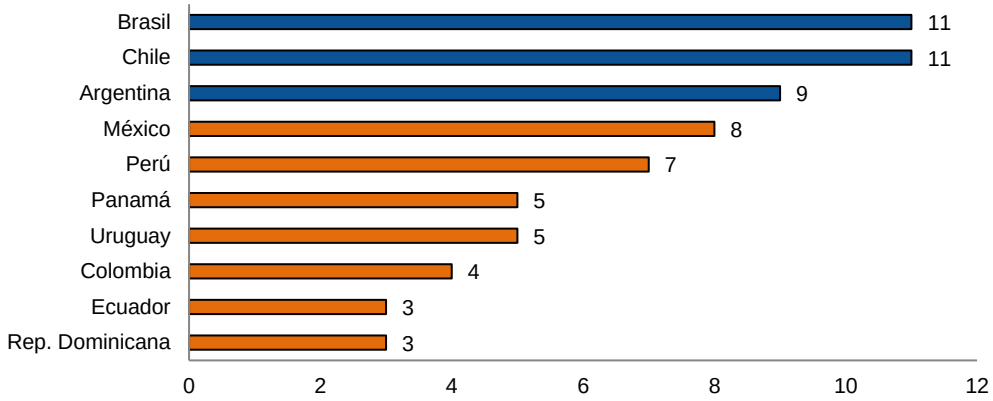
(2) 15/5/2017, Wanna Decryptor, el ransomware que aterrorizó al mundo también llega a México. https://www.xataka.com.mx. Recuperado en nov-20. Véase en línea: https://www.xataka.com.mx/ aplicaciones/wanna-decryptor-el-ransomware-que-aterrorizo-al-mundo-tambien-llego-a-mexico.

(3) 13/5/2017, Petrobras tambiem, alvo do ataque global de hackers. https://www.sindipetroprsc.org.br/. Recuperado en nov-20. Véase en línea: https://www.sindipetroprsc.org.br/site/index.php/ noticias/item/2932-petrobras-tambem-e-alvo-do-ataque-global-de-hackers.

(4) 31/5/2017, Un ciberataque global dejó dos puertos de nuestra región sin poder operar. https://www.sapei.com.ar/. Recuperado en nov-20. Véase en línea: https://www.sapei.com.ar/website/category/ noticias--/477-un-ciberataque-global-dejo-dos-puertos-de-nuestra-region-sin-poder-operar;jsessionid=3420A364DF08C105DD4A7946A0A845DA.
(5) 29/6/2017, Hackean sistema de empresa portuaria en Michoacán. https://www.elsoldemexico.com.mx/. Recuperado en nov-20. Véase en línea: https://www.elsoldemexico.com.mx/ republica/justicia/hackean-sistema-de-empresa-portuaria-en-michoacan-147426.html.
(6) 16/8/2017, Maersk calcula en USD 300 millones p,rdidas generadas por ciberataque. https://portalportuario.cl/. Recuperado en nov-20. Véase en línea: https://portalportuario.cl/maersk-calcula-usd-300-millones-perdidas-generadas-ciberataque/.
(7) 29/6/2017, Terminales del Muelle Norte del Puerto del Callao sufrieron ataque cibernético. https://www.apam-peru.com/web/. Recuperado en nov-20. Véase en línea: https://www.apam-peru.com/web/terminales-del-muelle-norte-del-puerto-del-callao-sufrieron-ataque-cibernetico/.
(8) 30/6/2017, Un ciberataque global dejó dos puertos de nuestra región sin poder operar. https://www.sapei.com.ar/. Recuperado en nov-20. Véase en línea: https://www.sapei.com.ar/ website/category/noticias--/477-un-ciberataque-global-dejo-dos-puertos-de-nuestra-region-sin-poder-operar;jsessionid=3420A364DF08C105DD4A7946A0A845DA.
(9) 28/12/2017. La naviera Clarksons víctima de un ciberataque. https://blog.intec2.com/. Recuperado en nov-20. Véase en línea: https://blog.intec2.com/2017/12/la-naviera-clarksons-victima-de-un.html.
(10) 7/9/2020. Banco de Estado Chileno víctima ataque ransomware Revil: cajeros cerrados. https://blog.elhacker.net/. Recuperado en nov-20. Véase en línea: https://blog.elhacker.net/2020/09/banco-de-estado-chile-victima-de-ransomware-Revil-Sodinokibi.html.
(11) 10/6/2018. Banco de Chile, virus para distraer y luego robo por 10 Millones de dolares en la red SWIFT, 24 de Mayo. https://cesarfarro.medium.com/banco-de-chile-robo-por-m%C3%A1s-de-10-millones-de-d%C3%B3lares-el-24-de-mayo-4a3511afc956. Recuperado en 11-20. Véase en línea: https://cesarfarro.medium.com/banco-de-chile-robo-por-m%C3%A1s-de-10-millones-de-d%C3%B3lares-el-24-de-mayo-4a3511afc956.
(12) 17/7/2018. Fedex afectado por el ataque del ransomware Petya. https://www.clasesordenador.com/. Recuperado en nov-20. Véase en línea: https://www.clasesordenador.com/fedex-afectado-por-el-ataque-ransomware-petya/.
(13) 30/7/2018. Operaciones de Cosco en América vuelven a la normalidad tras ciberataque. https://portalportuario.cl/. Recuperado en nov-20. Véase en línea: https://portalportuario.cl/operaciones-de-cosco-en-america-vuelven-a-la-normalidad-tras-ciberataque/.
(14) 24/8/2018. Crónica del ciberataque a entidades bancarias peruanas. https://www.optical.pe/. Recuperado nov-20. Véase en línea: https://www.optical.pe/blog/cronica-del-ciberataque-a-entidades-bancarias-peruanas/.
(15) 4/2/2019. Secuestro virtual y rescate en bitcoins: la historia detrás del ciberataque a una cooperativa en Esquel. https://www.lanacion.com.ar/. Recuperado en nov-20. Véase en línea: https://www.lanacion.com.ar/tecnologia/secuestro-virtual-rescate-bitcoins-historia-detras-del-nid2216640/.
(16, 17, 18 y 19) 2/7/2019. Chile: ciberataque a Minagri y virus informático en sistemas de Ultramar. https://diemmatotal.over-blog.com/. Recuperado en nov-20. Véase en línea: https://diemmatotal.over-blog.com/2019/07/chile-ciberataque-a-minagri-y-virus-informatico-en-sistemas-de-ultramar.html.
(20) 10/11/2019. El rescate por el hackeo a Pemex es el segundo mayor por ransomware. https://www.eleconomista.com.mx/. Recuperado en nov-20. Véase en línea: https://www.eleconomista.com.mx/empresas/El-rescate-por-el-hackeo-a-Pemex-es-el-segundo-mayor-por-ransomware-20191115-0035.html.
(21) 16/3/2020. Cosan: interrupção em sistemas operacionais ocorreu devido a ataque de hackers. https://www.istoedinheiro.com.br/. Recuperado en nov-20. Véase en línea: https://www.istoedinheiro.com.br/cosan-interrupcao-em-sistemas-operacionais-ocorreu-devido-a-ataque-de-hackers/.
(22) 1/4/2020. Informe 2019 - Hacktivismo y Ciberyidhadismo CNN-CERT IA - 04/20. https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/. Recuperado en nov-20. Véase en línea: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4714-ccn-cert-ia-04-20-informe-anual-2019-hactivismo-y-ciberyihadismo-1/file.html.
(23) 13/4/2020. Sospecha de ciberataque contra MSC. http://rm-forwarding.com/. Recuperado en nov-20. Véase en línea: http://rm-forwarding.com/2020/04/13/sospecha-de-ciberataque-contra-msc/.
(24) 9/10/2020. Aumentan ciberataques contra empresas de hidrocarburos y servicios públicos. https://www.bnamericas.com/es/. Recuperado en nov-20. Véase en línea: https://www.bnamericas.com/es/noticias/aumentan-ciberataques-contra-empresas-de-hidrocarburos-y-servicios-publicos.
(25) 30/6/2020. Ransomware Maze anuncia invasão nas redes da CPFL e outras empresas. https://minutodaseguranca.blog.br/. Recuperado en nov-20. Véase en línea: https://minutodaseguranca.blog.br/ransomware-maze-anuncia-invasao-nas-redes-da-cpfl-e-outras-empresas/.
(26) 30/7/2020. Garmin admite un ciberataque por ®ransomware¯ que dejó inactivos a sus usuarios durante cinco días. https://www.abc.es/tecnologia/redes/abci-garmin-admite-ciberataque-ransomware-dejo-inactivos-usuarios-durante-cinco-dias-202007280938_noticia.html. Recuperado en nov-20. Véase en línea: https://www.abc.es/tecnologia/redes/abci-garmin-admite-ciberataque-ransomware-dejo-inactivos-usuarios-durante-cinco-dias-202007280938_noticia.html.
(27) 17/8/2020. Banco en M,xico sufre otro ataque ransomware, pero niega filtración de datos. https://www.criptonoticias.com/. Recuperado en nov-20. Véase en línea: https://www.criptonoticias.com/seguridad-bitcoin/banco-mexico-sufre-ataque-ransomware-niega-filtracion-datos/.
(28) 1/10/2020. CMA CGM sospecha brecha de datos como consecuencia de ataque cibernético. https://www.mundomaritimo.cl/. Recuperado en nov-20. Véase en línea: https://www.mundomaritimo.cl/noticias/cma-cgm-sospecha-brecha-de-datos-como-consecuencia-de-ataque-cibernetico.
(29) 12/10/2020. CMA CGM vuelve a la normalidad tras dos semanas desde ciberataque. https://www.mascontainer.com/. Recuperado en nov-20. Véase en línea: https://www.mascontainer.com/cma-cgm-vuelve-a-la-normalidad-tras-dos-semanas-desde-ciberataque/.
(30) 8/10/2020. Braskem, alvo de hackers e declara for‡a maior. https://valorinveste.globo.com/. Recuperado en nov-20. Véase en línea: https://valorinveste.globo.com/mercados/renda-variavel/empresas/noticia/2020/10/08/braskem-e-alvo-de-hackers-e-declara-forca-maior.ghtml.

Respecto a los países afectados por los eventos relevados, Brasil y Chile encabezan la lista, continuando en orden Argentina, México, Perú, Panamá, Uruguay, Colombia, Ecuador y República Dominicana.

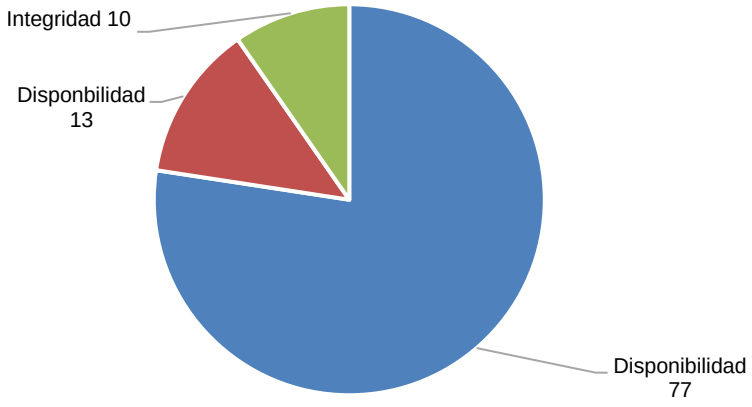
Gráfico 3
Paises afectados por cantidad de incidentes



Fuente: Elaboración basada en información obtenida a través de la encuesta aplicada por CEPAL.

Al mismo tiempo se verifica que en la mayoría de los casos, los incidentes registrados han afectado el pilar de la ciberseguridad que tiene mayor impacto en logística: la disponibilidad. En el 77,4 % de los casos las organizaciones que fueron víctimas de los ataques, tuvieron disrupciones tecnológicas que impactaron en sus procesos, y el tiempo promedio en el que estas instituciones debieron prescindir de los sistemas comprometidos fue de 7 días. En nivel de impacto, continúa la confidencialidad con un 12,9% de los casos y un 9,7% de los casos han atentado contra la integridad de la información (gráfico 4).

Gráfico 4
Impacto en la organización
(En porcentajes)



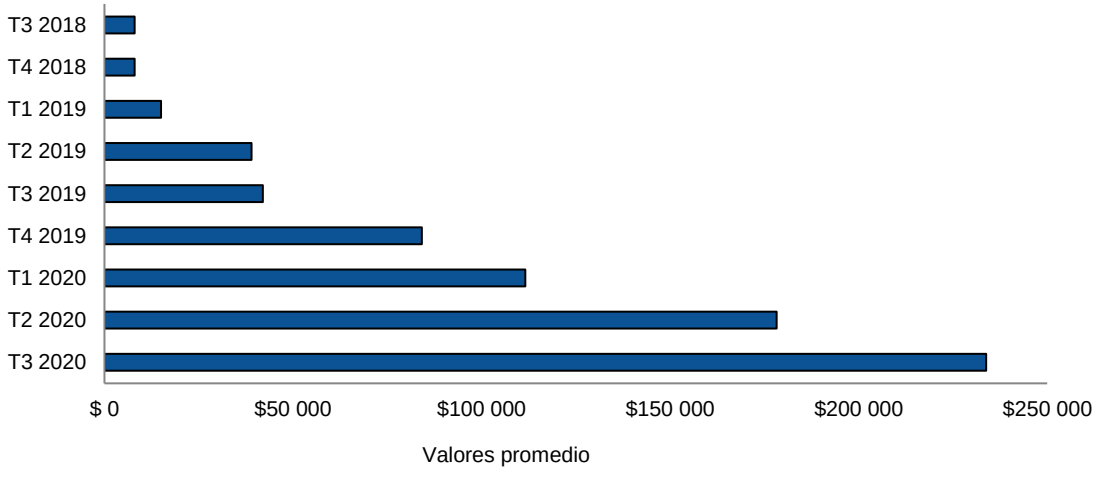
Fuente: Elaboración basada en información obtenida a través de la encuesta aplicada por CEPAL.

Esta distribución que se ha armado en función del principal impacto de los incidentes ocurridos en los últimos 5 años, está cambiando durante 2020 a partir de la aparición de ataques combinados de ransomware, donde los datos se exportan a manos del atacante antes de ser encriptados, vulnerando de esta manera la confidencialidad de la información capturada y la disponibilidad de los sistemas que se encriptaron durante los ataques, por lo tanto, en el futuro habrá mucho más riesgo de exposición de datos de las organizaciones vulneradas. En la logística de América Latina, el 50 % de los ataques denunciados corresponden a ransomware, encontrándose además que durante el año 2020, el promedio de los rescates solicitados se ha triplicado respecto a 2019, solicitándose el rescate económico ya no solo para recuperar la operatividad, sino también para no exponer públicamente los datos capturados (Sophos, 2020).

II. La evolución del ransomware

El *ransomware Maze*, que entró en actividad a finales del año 2019, es el primer tipo de *malware* que ha operado de forma tal que la organización, detrás del mismo, no solo extorsiona a sus víctimas para devolver la operación a la normalidad, sino también para no divulgar la información secuestrada.

Gráfico 5
Rescate promedio por trimestre
(En dólares)



Fuente: Elaboración propia basada en datos obtenidos de Coveware, https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority.

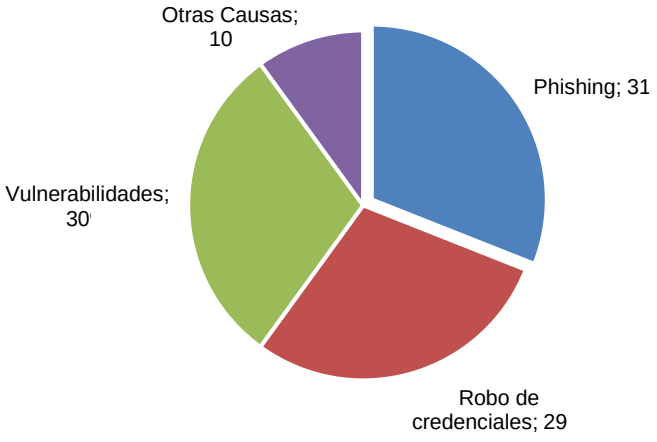
.

En la modalidad, le continuaron DopplePaymer, Sodinokibi, Netwalker, Conti y Egregor. En la evolución de esta modalidad, se puede observar en aumento la velocidad de difusión y los montos de rescate solicitados. A modo de ejemplo de la aceleración en la velocidad de difusión, se puede mencionar que Maze ha conseguido que 50 víctimas paguen el rescate en 6 meses de ataques, en tanto su sucesor más reciente Egregor, que logró tomar como víctima a Cencosud en noviembre de 2020, consiguió el mismo objetivo en solo 3 semanas. Las cifras solicitadas en los rescates se han elevado rápidamente a partir del momento en el que los ciber atacantes descubrieron que, por un lado, logran más eficacia en la monetización amenazando con divulgar información cuya privacidad tiene un valor muy elevado, especialmente en casos donde los datos secuestrados están bajo el amparo de leyes de protección de datos personales, y por otro lado, que las técnicas y tácticas utilizadas para vulnerar a una organización pequeña o mediana no difieren sustancialmente de las necesarias para empresas de mayor tamaño que potencialmente pueden afrontar pagos sensiblemente más elevados. Conforme la efectividad del cobro del rescate fue creciendo, fueron también elevándose en promedio los valores de los rescates solicitados, llegando en el tercer trimestre de 2020 a triplicar los montos del cuarto trimestre del año anterior (Coveware, 2020).

III. Análisis de las causas de los incidentes

Cuando se investiga la causa raíz de los incidentes de ciberseguridad, los tres principales vectores pertenecen a phishing con 31% de casos, 30% escaneo y explotación de vulnerabilidades, y 29% robo de credenciales de acceso (Symantec, 2019). Es decir que el 60% corresponden a debilidades que tienen origen en la preparación de las personas para el uso de la tecnología, ya sea por falta de reconocimiento de un email engañosos o por el uso de contraseñas débiles o iguales en múltiples sitios.

Gráfico 6
Causas de los incidentes
(En porcentajes)



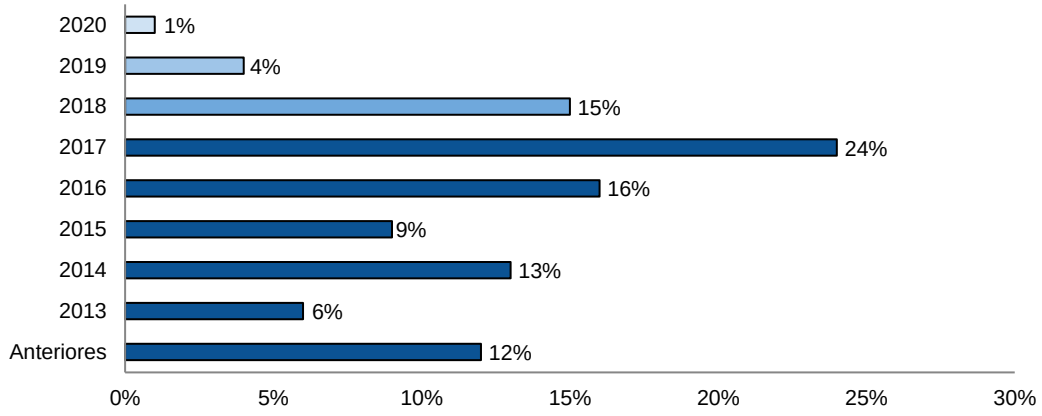
Fuente: Elaboración propia basada en datos de Internet Security Threat Report 2019 – Symantec.

Cuando las causas corresponden a robo de credenciales, en general la vía que se utiliza para acceder a la organización es el protocolo nativo que tienen los sistemas operativos para permitir el

trabajo de manera remota. En el caso de la firma Microsoft, se denomina *Remote Desktop Protocol* (RDP), y si bien se venía utilizando por las ventajas operativa que permite esta modalidad, fue un recurso que algunas organizaciones utilizaron en mayor cantidad para permitir el trabajo de sus colaboradores durante los períodos de aislamiento que ocurrieron durante la pandemia.

Al analizar las vulnerabilidades explotadas en el primer semestre de 2020 utilizadas como vector de ataque, se ha encontrado que solo el 5% corresponden a vulnerabilidades descubiertas en los años 2019 y 2020, y solo un 15% en 2018. Es decir que el 80% de las vulnerabilidades explotadas llevaban al menos 2 años conocidas públicamente y existían actualizaciones para poder repararlas (Checkpoint, 2020). Estas cifras exponen las dificultades que las organizaciones tienen a la hora de mantener los sistemas operativos de sus equipos actualizados para corregir vulnerabilidades descubiertas, dando a los atacantes mayor tiempo para desarrollar los paquetes capaces de explotarlas, y mayor vida útil a dichos paquetes.

Gráfico 7
Antigüedad de vulnerabilidades explotadas
(En porcentajes)



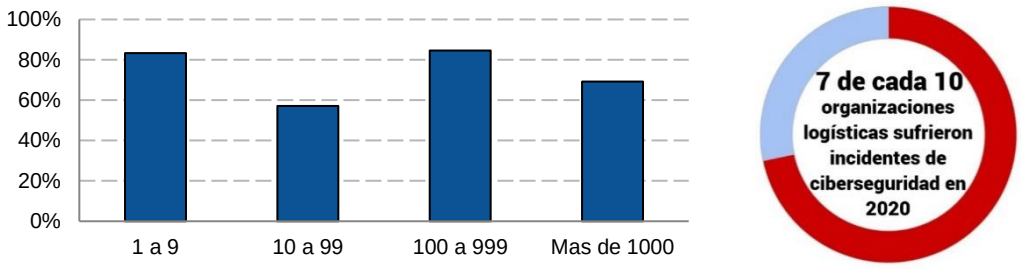
Fuente: Cyber attack trends: 2020 mid-year report -Check Point.

IV. La realidad de las organizaciones de logística puertas adentro

Si bien los niveles de ciberseguridad han mejorado en los últimos años en la región de América Latina, la mayoría de los estados registran un nivel **inicial** dentro del Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM), elaborado por la Universidad de Oxford (BID y OEA, 2020). En este contexto, y ante la escasez de denuncias o divulgaciones públicas que ayuden a las organizaciones relacionadas con la logística a mejorar su nivel de madurez individual, y por ende a ayudar a elevar el nivel colectivo, se ha realizado una encuesta en la que participaron instituciones públicas y privadas de dicho ámbito. A continuación, se transcriben las principales conclusiones.

El **72% de las organizaciones cuentan con al menos un incidente de ciberseguridad en los últimos 12 meses**. Culturalmente en LAC se cree que los incidentes aumentan conforme aumenta el tamaño de la organización, situación que se descarta en varios estudios a nivel global y regional, y confirma la distribución de la encuesta, en la cual no se verifican tendencias en que los ataques sean dependientes del tamaño de la organización.

Gráfico 8
Distribución por tamaño de organización
(En porcentajes)

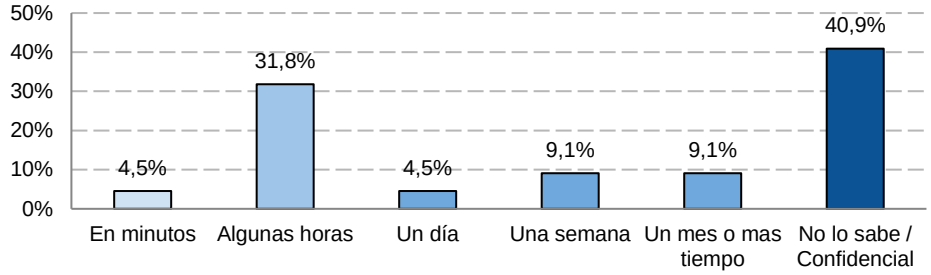


Fuente: Elaboración basada en información obtenida a través de la encuesta aplicada por CEPAL.

Llama la atención que solo el 50% de las organizaciones están preocupadas por los incidentes que pueden ocurrir dentro de los próximos 12 meses, sin importar el tamaño de la organización o si sufrieron incidentes de ciberseguridad en el pasado reciente. Esta tendencia es consecuente con el nivel de madurez del modelo CMM regional y con la necesidad de compartir datos reales a través de instituciones públicas regionales. Dicho en otras palabras, muchas organizaciones al ser vulneradas y consultar con colegas, no encuentran la respuesta que posibilite compartir experiencias para poder afrontar el tratamiento desde una modalidad evolutiva regional, sino solamente con la preparación individual de las organizaciones y sus miembros. Esto resulta en que se pueda tratar a los incidentes, dependiendo exclusivamente del procedimiento pre-crisis o estado de resiliencia que cada uno haya desarrollado en el *deber hacer.* Además, el estado actual de madurez, hace que las economías más pequeñas puedan sufrir consecuencias relativamente superiores a quienes pueden contar con mejores mecanismos de defensa propios.

El 40,9% de las instituciones consultadas que sufrieron un incidente de seguridad en los últimos 12 meses, **no pueden precisar el tiempo que les llevó normalizar la situación** luego del incidente. Si bien apenas el 4,5% pudo resolver el incidente en minutos, al 54,5% les llevó desde algunas horas hasta más de un mes de esfuerzo retomar la operación habitual.

Gráfico 9
Tiempo de recuperarse de un incidente
(En porcentajes)

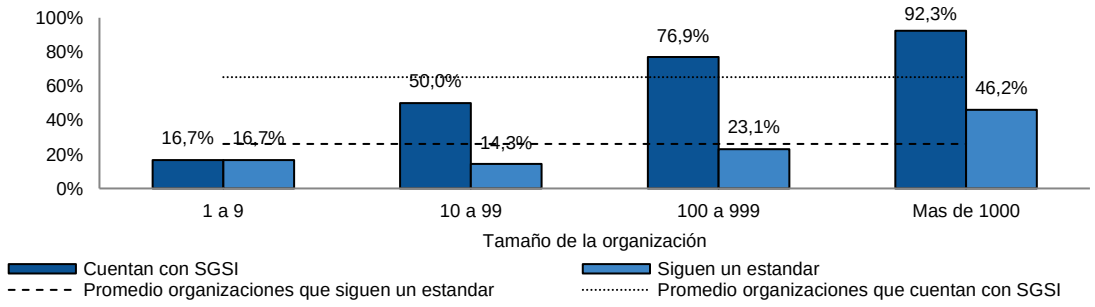


Fuente: Elaboración basada en información obtenida a través de la encuesta aplicada por CEPAL.

.

Al consultar sobre el nivel de formalización de la seguridad, el 65,2% de las organizaciones cuentan actualmente con una política que es parte de un plan de gestión de ciberseguridad en el cual confían con un nivel moderado a elevado. Sin embargo solo el 26,1% basan sus normas y procedimientos en un estándar como guía, siendo la norma ISO/IEC 27.001 la guía elegida en la mayoría de los casos.

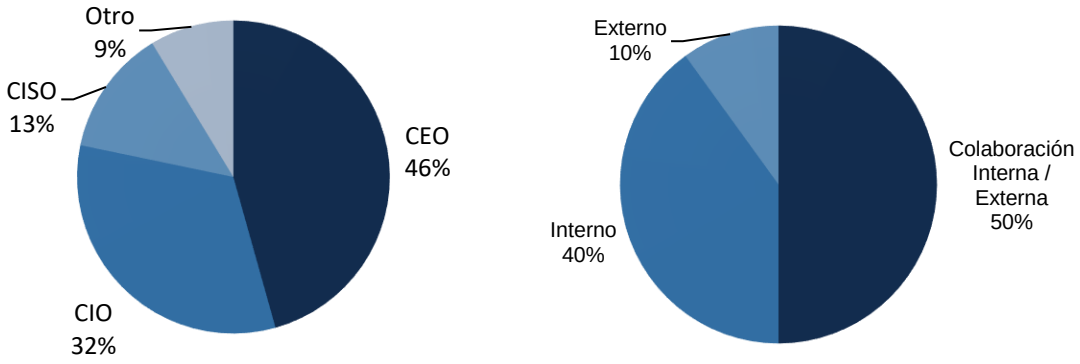
Gráfico 10
Formalización de la gestión de la ciberseguridad
(En porcentajes)



Fuente: Elaboración basada en información obtenida a través de la encuesta aplicada por CEPAL.

Al evaluar las estructuras organizativas en materia de seguridad, en logística y las instituciones relacionadas con el rubro en LAC, el 15,2% cuenta con una estructura independiente para atender las necesidades de ciberseguridad, siendo atendidas en un 45,7% de las organizaciones por el Director Ejecutivo y en el 32,6% de los casos por la autoridad máxima del área de sistemas de información. Dichos funcionarios, al momento de resolver las tareas de gestión y operativas de ciberseguridad, conforman los equipos de trabajo con colaboración entre personal propio y organizaciones externas en el 50% de los casos. En el 40% de las organizaciones encuestadas, las tareas se realizan con personal interno, mientras que el 10% delegan las tareas totalmente en empresas de terceras partes.

Gráfico 11
Estructura organizativa para la gestión de la seguridad
(En porcentajes)

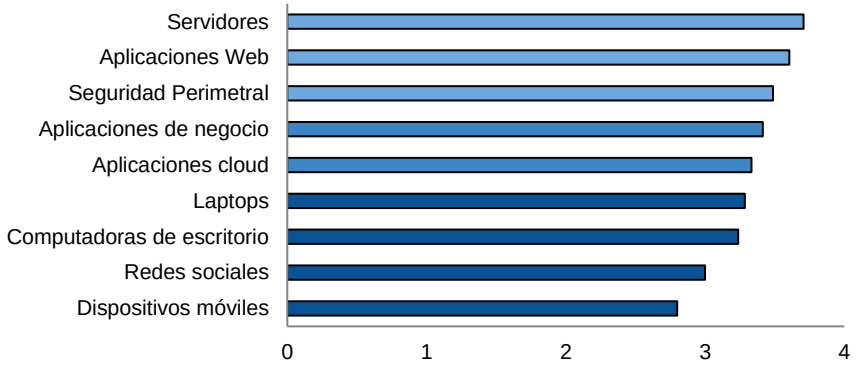


Fuente: Elaboración basada en información obtenida a través de la encuesta aplicada por CEPAL.

V. Una mirada técnica de la situación actual

En cuanto al nivel de confianza sobre las medidas actualmente implementadas en diferentes tecnologías, las que generan el mayor nivel de confianza son aquellas donde la gestión técnica del área de sistemas de información tiene mayor impacto, y donde, históricamente, se implementaron controles y medidas para reducir el riesgo. Es el caso de los servidores propios, aplicaciones web y seguridad lógica perimetral. Cuentan con menor confianza, las tecnologías donde los usuarios finales tienen mayor influencia, como, por ejemplo, las computadoras personales, el uso de redes sociales y los teléfonos móviles.

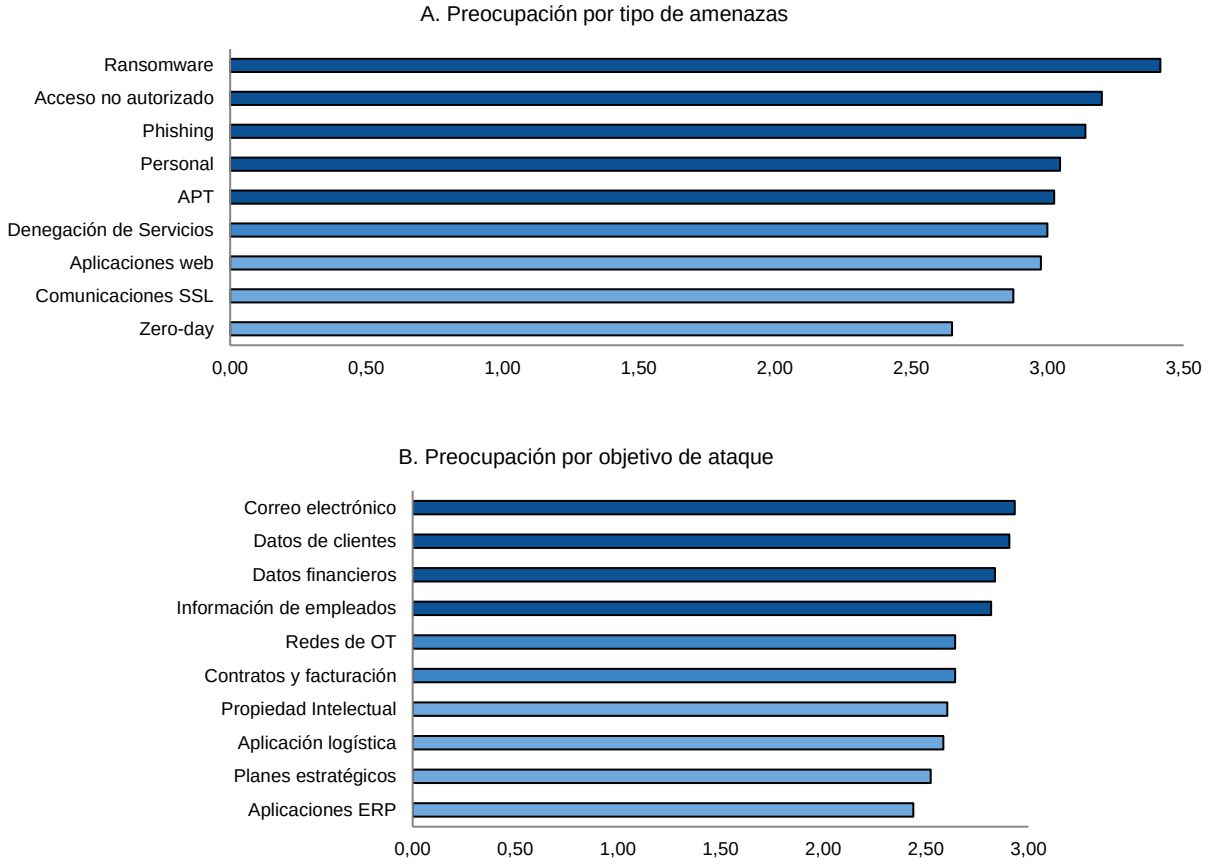
Gráfico 12
Nivel de confianza en los controles de ciberseguridad implementados



Fuente: Elaboración basada en información obtenida a través de la encuesta aplicada por CEPAL.

Al analizar las preocupaciones existentes sobre los tipos de ataques y los activos a proteger, se encuentran consistencias con los eventos ocurridos hasta el presente. Las amenazas que más preocupan son el ransomware, el acceso no autorizado, mediante contraseñas robadas (el *phishing).*

Gráfico 13
Preocupación por tipo de amenazas y por objeto de ataque
(Escala 1 a 5 siendo 6 la mayor preocupación)



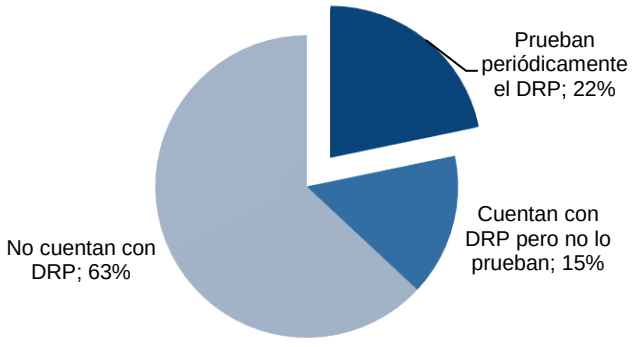
Fuente: Elaboración basada en información obtenida a través de la encuesta aplicada por CEPAL.

En cuanto a los activos, la mayor preocupación se centra en la información de correo electrónico y en los datos de terceros que se reciben en custodia.

VI. Prácticas sobre resiliencia cibernética

En el boletín FAL número 382 de la CEPAL titulado *"La ciberseguridad en tiempos del COVID-19 y el tránsito hacia una ciberinmunidad"*, se ha desarrollado el concepto sobre la visión de ciberinmunidad, donde se explica que en una práctica en la cual el nivel de riesgo nunca puede eliminarse por completo, recibir un ataque, matemáticamente es solo una función dependiente del tiempo, definición que motiva a que los equipos de trabajo tengan documentación y ejerciten las posibles salidas de servicio. Al consultar en la encuesta sobre esta práctica, solo el 37% de las organizaciones cuentan con un procedimiento de recuperación ante desastres, comúnmente llamado DRP por las siglas en inglés (disaster recovery plan), pero apenas el 22% realizan pruebas periódicas que le permiten afrontar una situación real de crisis de manera más efectiva.

Gráfico 14
Organizaciones que cuenta con DRP
(En porcentajes)



Fuente: Elaboración basada en información obtenida a través de la encuesta aplicada por CEPAL.

En regiones donde las organizaciones se encuentran en etapas avanzadas del CMM y se evalúan los riesgos de manera más asertiva, la adquisición de pólizas de cobertura por los posibles daños por ciberataques aumenta de manera ininterrumpida a una tasa de 25% por año, pasando de 200 reclamos en 2017 a 800 en 2019 (Allianz, 2020). El dimensionamiento de las coberturas se encuentra relacionado con el nivel de dependencia tecnológica que cada organización tenga según su actividad principal, y el grado de afectación que pudieran tener sus procesos secundarios, como así también del impacto que pudieran sufrir las terceras partes, pudiendo ser estas otras organizaciones o individuos.

El crecimiento del sector del mercado de seguros deviene por el aumento de la demanda de pólizas para ciberdelitos y la consecuente oferta surgida satisfaciendo sus expectativas. Se produce entonces un fenómeno de "retroalimentación" que aumenta la confianza entre los integrantes de los diferentes pasos de la cadena logística, no solo por la asistencia que las pólizas dan en la aparición de un incidente, lo cual ayuda a recuperarse más rápidamente, sino por el proceso en sí que las aseguradoras solicitan en sus condiciones de contratación Cabe destacar que este proceso es la resultante de las necesidades de los actores de la cadena logística y de la acertada respuesta de los proveedores del servicio, por lo que se ha adoptado de manera similar al que se haría con un cumplimento regulatorio o un estándar de facto (Aspen US Holdings, 2020).

VII. Ciberinmunidad, una estrategia de ciberseguridad para la recuperación pospandemia

Los registros encontrados en la investigación y las opiniones recolectadas de las instituciones que participaron del relevamiento realizado por CEPAL arrojan resultados que sugieren contar con un plan o estrategia de ciberseguridad que acompañe el camino hacia una logística basada en los nuevos paradigmas de la Industria 4.0, y faciliten a la región la posible recuperación de su operatividad pospandemia de manera competitiva. Las organizaciones consultadas han respondido sobre lo que imaginan para los próximos 12 meses, una aceleración de la digitalización de la economía, con un crecimiento promedio del **34%** en tecnologías disruptivas y en consecuencia los activos digitales podrían estar más expuestos a ser atacados, sobre todo siendo la industria del cibercrimen un rubro que crece lucrativamente con pronóstico de alcanzar los US$ 6000 millones para el año 2021 (Cybersecurity Ventures,2020) , en una economía global en recesión.

Las variables analizadas sugieren que la elaboración de un plan sería mucho más efectiva trascendiendo fronteras, como también lo hace la información. Si bien algunos países como Uruguay y Colombia arrojan indicadores de un nivel de madurez por encima del promedio en materia de ciberseguridad como consecuencia de planes estratégicos locales (BID y OEA, 2020), la naturaleza tecnológica a abordar, requiere una acción colaborativa regional, no solo en el marco legislativo, para facilitar las investigaciones internacionales que pudieran derivar de los incidentes, sino también para favorecer la cooperación en las acciones preventivas que puedan derivar del análisis en tiempo real de la actividad del ciberdelito en la región. La adhesión de algunos países a la Convención de Budapest como marco internacional de cooperación en la lucha contra el delito informático, parece ser un camino adecuado para coordinar las acciones de investigación y legales. En tal dirección, República Dominicana es quien suscribió en primer lugar a la convención en el año 2013, logrando en la actualidad un nivel de madurez 4 del modelo CMM en el ámbito legislativo como consecuencia de dicha decisión estratégica.

En todos los casos, la experiencia recolectada por los países pioneros de LAC para desarrollar estrategias o actividades relacionadas con la ciberseguridad, debería ser analizada para acelerar la adopción de medidas de aquellos que aún no cuentan con las herramientas.

Si bien las acciones en ámbitos de la administración pública suelen ser más efectivas a largo plazo, las organizaciones que forman parte de la cadena logística y aquellas que forman parte de la infraestructura crítica de las naciones, deberían contar con un Sistema de Gestión de Seguridad de la Información (SGSI), acciones prácticas basadas en estándares internacionales para aumentar su resiliencia operativa.

Como posibles estrategias para la evolución de la cibercultura regional, se proponen los siguientes lineamientos:

- Aquellos estados que aún no cuentan con su NCS, deberían comenzar por esta definición para asignar prioridades y recursos, de manera que los esfuerzos posteriores estén alineados con esta estrategia.

  El capital humano debería ser el factor fundamental para la transformación cultural que requiere el tránsito hacia la ciberinmunidad, por lo tanto, la **incorporación de contenidos cognitivos adecuados en los ámbitos educativos de todos los niveles** puede ser un primer paso que las naciones deberían considerar.

  La incorporación en las currículas de contenidos como protección de datos personales, ayudaría a mejorar los niveles de madurez actuales en la protección de los derechos de los ciudadanos. La base sobre la que cada individuo puede elevar la comprensión sobre el valor que los datos tienen actualmente, representando los objetos del mundo físico, pero por sobre todo a los seres humanos. Promover la oferta educativa especializada de nivel terciario o de grado en ciberdefensa, y revisar las currículas de los contenidos actuales relacionados con las tecnologías de la información y comunicaciones, podría ser una buena estrategia desde la gestión pública de cada estado nacional, contribuyendo a la sinergia regional.

- Reforzar la agenda en ciberdefensa de las instituciones regionales puede ser una buena estrategia para que la totalidad de las naciones colaboren entre sí, y avanzar colectiva e individualmente en el modelo CMM. Considerando que el monitoreo continuo de la actividad cibernética en la región puede generar alertas tempranas para evitar ciberataques, desde este ámbito podría crearse una red de colaboración regional que permita aumentar la capacidad de correlación de eventos, aumentando de esta manera la detección temprana para inocular defensas en las organizaciones con mayor anticipación y a mayor escala.

- La creación de un marco regulatorio o el fortalecimiento en las naciones que ya cuenten con estas medidas, servirían para elevar el nivel de confianza en ciberseguridad entre los integrantes de la cadena logística. Un ejemplo de acción valioso que elevaría dicho nivel de confianza entre las partes intervinientes en toda la cadena de logística es ayudar a las organizaciones a contar con las medidas de mitigación del riesgo acordes a su dimensión y procesos basándose en el estándar ISO 27.001, indicando la necesidad de contar formalmente con un DRP y que este se pruebe al menos anualmente, para luego aplicar las mejoras emergentes de dicha prueba[1].

[1] En sintonía con las recomendaciones que la Organización Marítima Internacional (IMO) a través de su comunicación MSC.1/Circ.1526, sería conveniente la revisión del código de Protección de Buques e Instalaciones Portuarias (PBIP) con el fin de verificar que el mismo contemple situaciones relacionadas con sabotajes que podrían ocurrir a través del uso de técnicas de ciberataques actuales atentando contra las infraestructuras críticas alcanzadas por el mismo que podrían resultar en consecuencias de impacto regional e internacional.

- Crear oficinas de orden nacional de respuesta ante incidentes o concretamente CSIRT de gobierno, o mejorar la interacción de estos centros con las organizaciones tanto privadas como públicas, ya que en gran cantidad de los países de la región ya existen. Esto ayudaría a resolver eventos de ciberseguridad de manera colaborativa entre los dos ámbitos, al igual que al servicio que brindan actualmente las instituciones responsables de la seguridad pública. Por solo citar un ejemplo, en el caso particular de ser víctimas de un ransomware, la participación de una entidad entrenada en la forma de llevar adelante la recuperación y el rescate resultaría de mucho valor para bajar los tiempos de salida de servicio, y eventualmente si fuera necesario, definir el curso de acción de un rescate.
- Aumentar la concientización pública en ciberseguridad podría elevar el nivel general de inmunidad a los ciberataques. Algunos países de Latinoamérica cuentan con una baja difusión de las amenazas presentes en internet. Al mismo tiempo las organizaciones privadas aún no evidencian contar con una percepción de riesgo que sea consistente con la realidad. La preocupación promedio respecto a los incidentes de ciberseguridad para el 2021 es del 50%, la que pareciera ser baja si se considera que el 70% de las organizaciones tuvieron incidentes durante 2020. La divulgación de incidentes ocurridos mejoraría la percepción del riesgo, y posiblemente, las instituciones asignarían una mayor prioridad a sus estrategias preventivas contra ataques informáticos.
- A nivel individual, además de continuar con las tradicionales medidas de protección de perímetro tecnológico, adecuados respaldos de información, protección y actualización de los equipos de usuario final, las organizaciones deberían evaluar la incorporación de detección temprana de incidentes mediante el monitoreo en tiempo real del tráfico de datos en la red y con herramientas avanzadas para su análisis; idealmente con técnicas de inteligencia artificial, atendiendo los eventos de manera inmediata con un equipo de atención de incidentes, denominado comúnmente Centro de Operaciones de Seguridad (SOC por las siglas de su definición en inglés Security Operations Center). Al mismo tiempo limitar la expansión vertical de posibles incidentes mediante los modelos de defensa en capas, y laterales mediante el uso de microsegmentación de la red de datos.
- Es recomendable, en los proyectos de transformación tecnológica, considerar las implicancias de ciberseguridad desde la etapa inicial del proyecto, con las tareas apropiadas de diseño, definición e implementación distribuidas según corresponda con el proyecto tecnológico. Ver la ciberseguridad como una disciplina independiente, podría concluir en gastos y riesgos inesperados, y como consecuencia es esto último, retrasos en la puesta en marcha de dichos proyectos con las consecuencias que esto signifique.

En general, se debería continuar trabajando para fortalecer la ciberseguridad en la logística a nivel del marco institucional, regulatorio y de concientización colectiva e individual, sin perder el foco en las personas, que siguen siendo dos tercios de las causas de los incidentes de ciberseguridad. En simultáneo trabajar en crear o fortalecer los SGSI de las instituciones a nivel individual, con una perspectiva de resiliencia operativa para afrontar los desafíos tecnológicos de la Industria 4.0.

Bibliografía

Barleta, Pérez, Sánchez (2019), *La revolución industrial 4.0 y el advenimiento de una logística 4.0* - Boletín FAL 375, número 7, 2019, ISSN: 1564-4227, Santiago de Chile, Chile, 2019.

IDG (2020), *CIO COVID-19 Impact Study*. 30 de abril de 2020. Véase en línea en: https://www.idg.com/tools-for-marketers/cio-cv-19-impact-study/.

Clement, J (2020), *Coronavirus global online traffic impact as of October 2020* - noviembre 16, 2020. Véase en: https://www.statista.com/statistics/1105495/coronavirus-traffic-impact/#statisticContainer

_____ (2020), *Number of internet users worldwide from 2009 to 2020, by region* - octubre 9, 2020. Véase en: https://www.statista.com/statistics/265147/number-of-worldwide-internet-users-by-region/.

Sonicwall (2020), Sonicwall Security Center. Centro de recolección de eventos de la firma en: https://securitycenter.sonicwall.com/m/page/capture-labs-threat-metrics.

UIT (2018), *Guide to developing a national cybersecurity strategy - Strategic engagement in cybersecurity*, año: 2018. Véase en línea en: http://handle.itu.int/11.1002/pub/811cf62d-en.

NIST (2012), *Computer Security - Incident Handling Guide*. 2012. Véase en: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

Coveware (2020), *Ransomware Demands continue to rise as Data Exfiltration becomes common, and Maze subdues*, 4 de noviembre de 2020. Véase en: https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report.

Sophos (2020), *Informe de amenazas 2021 de Sophos*, noviembre 2020. Véase en línea en: https://www.sophos.com/es-es/medialibrary/PDFs/technical-papers/sophos-2021-threat-report.ashx

Symantec (febrero 2019), *ISTR - Internet Security Threat Report*; Symantec Corp., Mountain View, USA. Véase en: https://docs.broadcom.com/doc/istr-24-2019-e.

CheckPoint (Julio 2020), *Cyber attack trends: 2020 mid-year report*; Check Point Software Technologies Ltd., Tel Aviv, Israel. Véase en: https://research.checkpoint.com/2020/cyber-attack-trends-2020-mid-year-report/.

BID y OEA (agosto 2020), *Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe;* Banco Interamericano de Desarrollo, 26 de agosto de 2020. Véase en línea en: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-elcamino-a-seguir-en-America-Latina-y-el-Caribe.pdf.

Allianz (2020), *Cyber risk trends 2020*- año: 2020. Véase en línea en: https://www.agcs.allianz.com/news-and-insights/reports/cyber-risk-trends-2020.html.

Aspen US Holdings (2020), *Cyber risk and the evolution of supply chains*, año: 2020. Véase en línea en: https://www.aspen.co/globalassets/documents/insurance/Cyber-Risk-and-the-Evolution-of-Supply-Chains-ASPEN-Jun16.pdf.

FBI (2020), 2019 *Internet Crime Annual Report, Federal Bureau of Investigation*, US. Department of Justice, USA https://pdf.ic3.gov/2019_IC3Report.pdf.

Cybersecurity Ventures (2020), *The 2020 Official Annual Cybercrime Report*, Herjavec Group, Canada, https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/.

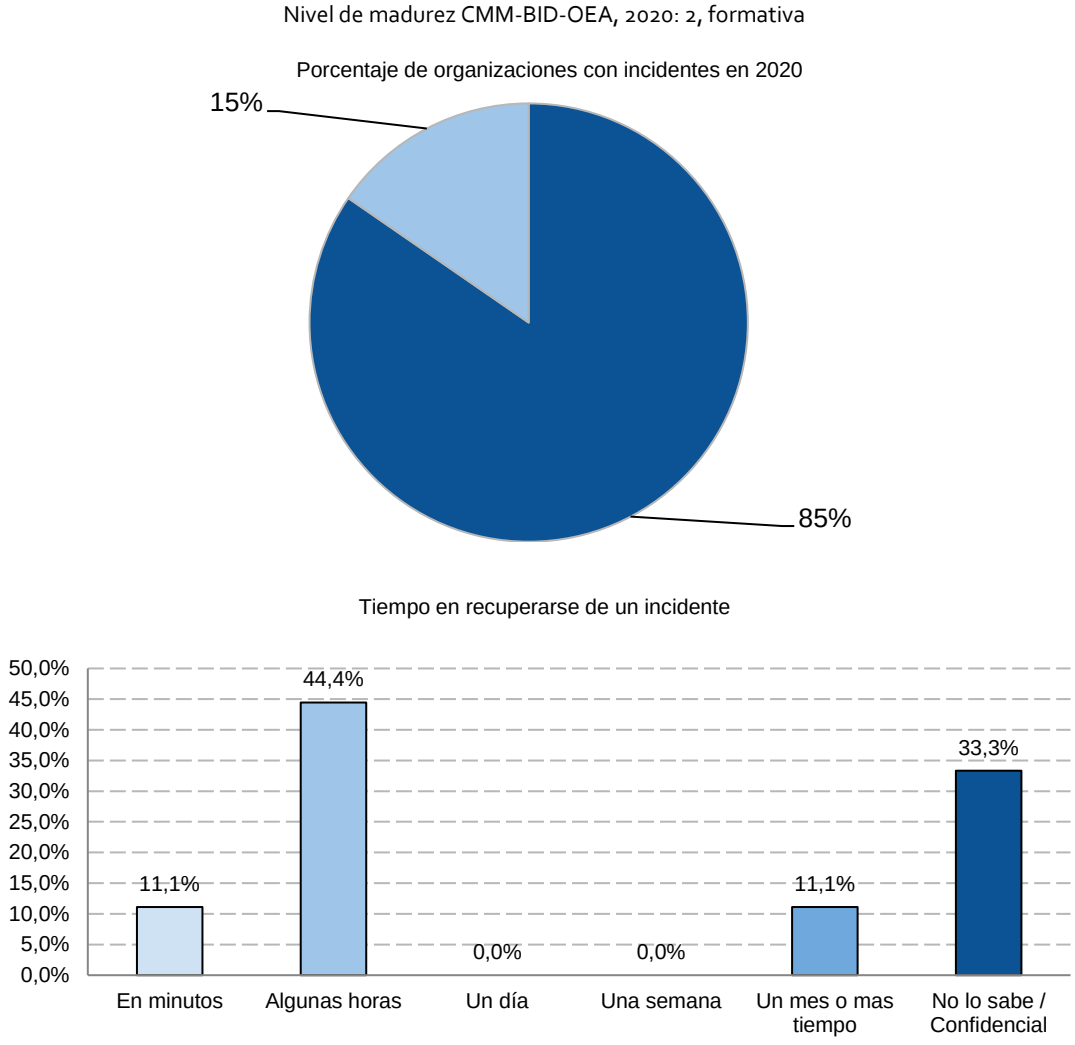
IMO (2016), *Guidance for the development of national maritime security legislation*. Véase en: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC.1-Circ.1525.pdf.

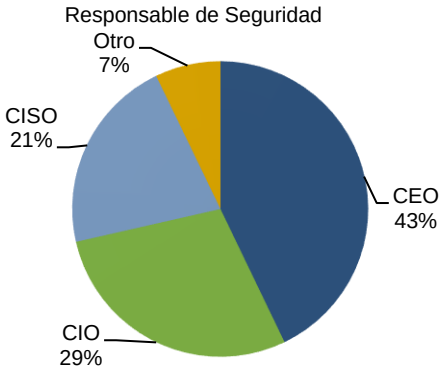
Anexos

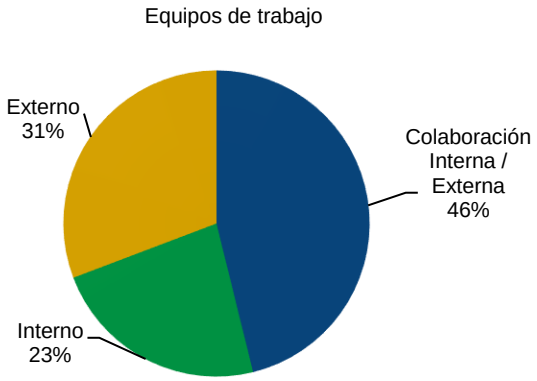
Anexo 1
Situación por país: Argentina

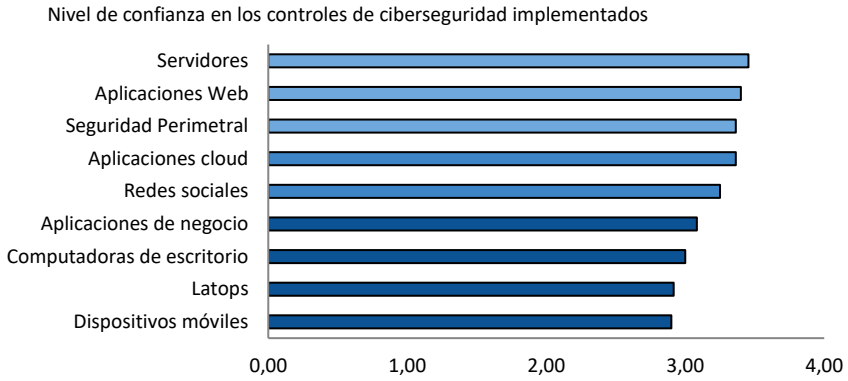
La evolución general de los índices del Reporte Ciberseguridad 2016-2020 es de tendencia positiva, pero es de señalar que los indicadores correspondientes al año 2020 promedian por debajo de la media esperada (2,09). Adicionalmente Argentina registra un avance en la creación de superestructura institucional que aún no se condice con el nivel de efectividad necesario.

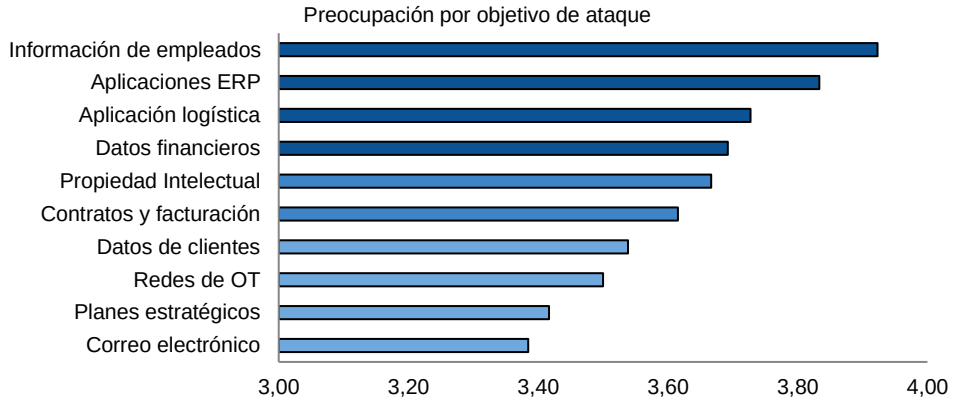
Grafico A1
Situación de Argentina
(En porcentajes)

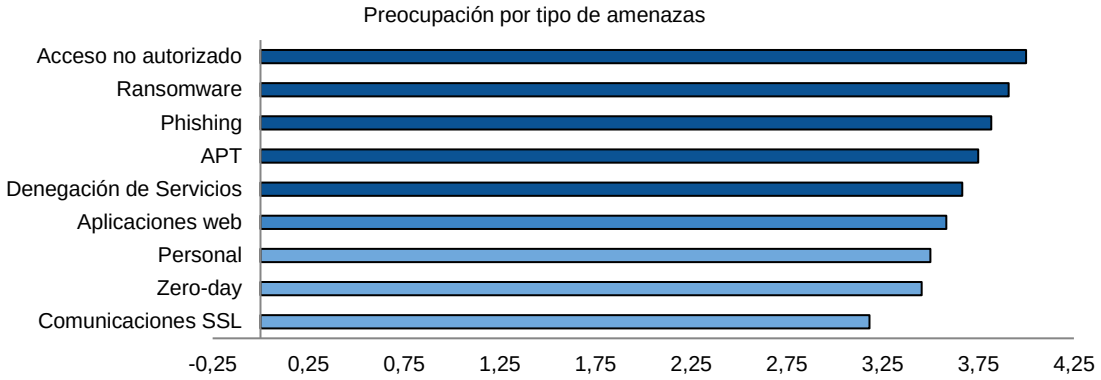


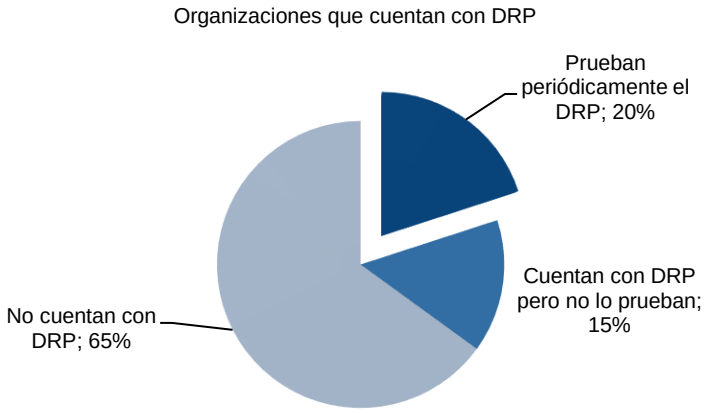

Responsable de Seguridad
Otro
7%
CISO
21%
CEO
43%
CIO
29%


Equipos de trabajo
Externo
31%
Colaboración
Interna /
Externa
46%
Interno
23%


Nivel de confianza en los controles de ciberseguridad implementados
Servidores
Aplicaciones Web
Seguridad Perimetral
Aplicaciones cloud
Redes sociales
Aplicaciones de negocio
Computadoras de escritorio
Latops
Dispositivos móviles
0,00
1,00
2,00
3,00
4,00


Preocupación por objetivo de ataque
Información de empleados
Aplicaciones ERP
Aplicación logística
Datos financieros
Propiedad Intelectual
Contratos y facturación
Datos de clientes
Redes de OT
Planes estratégicos
Correo electrónico
3,00
3,20
3,40
3,60
3,80
4,00



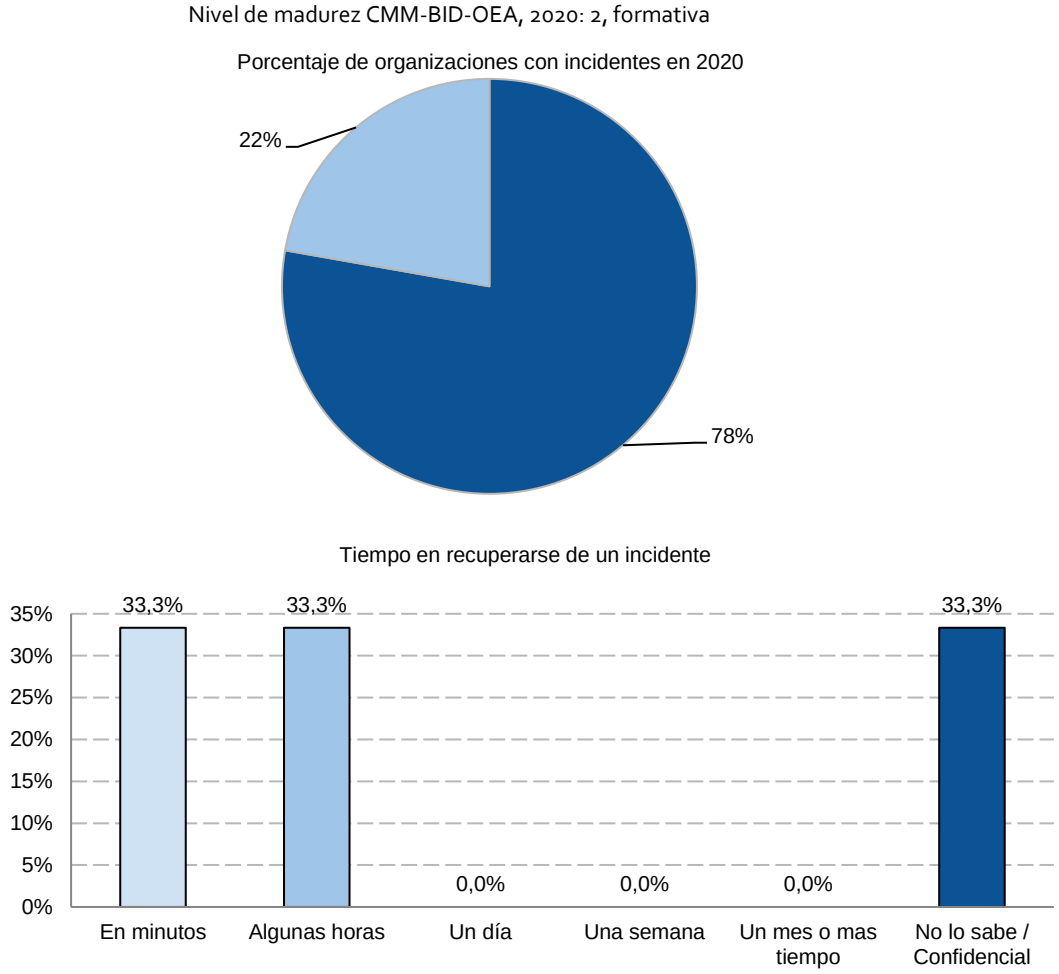


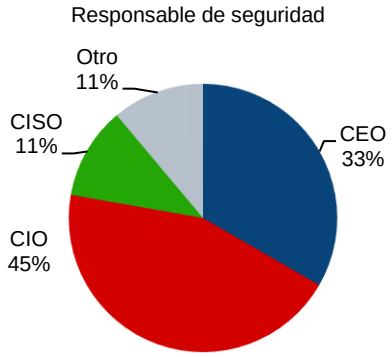
Fuente: Elaboración basada en información obtenida a través de la encuesta aplicada por CEPAL.

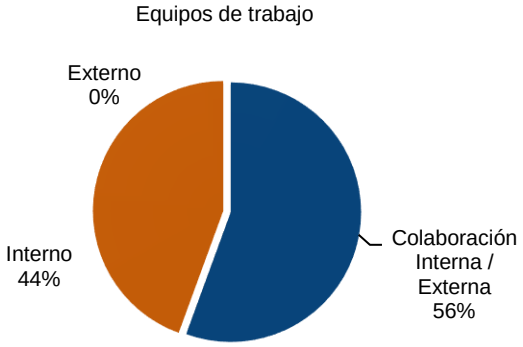
Anexo 2
Situación por país: Brasil

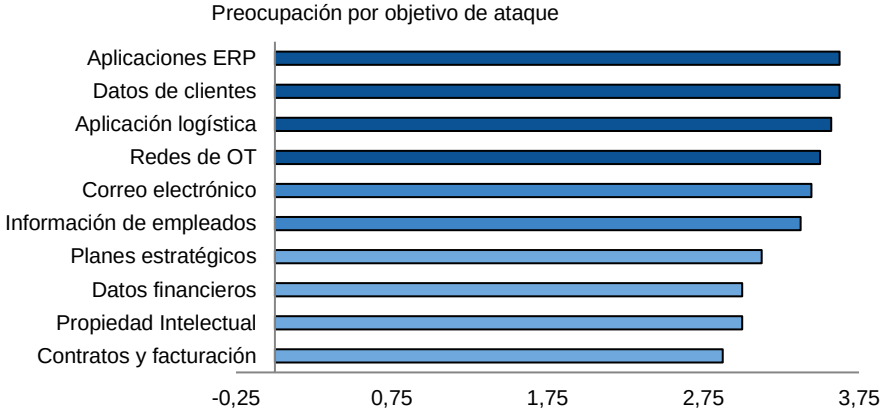
La política y Estrategia de Seguridad Cibernéticas son sus mayores fortalezas, junto con el desarrollo de infraestructura en cuanto a capacidad de respuesta para afrontar y resolver incidentes cibernéticos combinado con un buen nivel de madurez cultural.

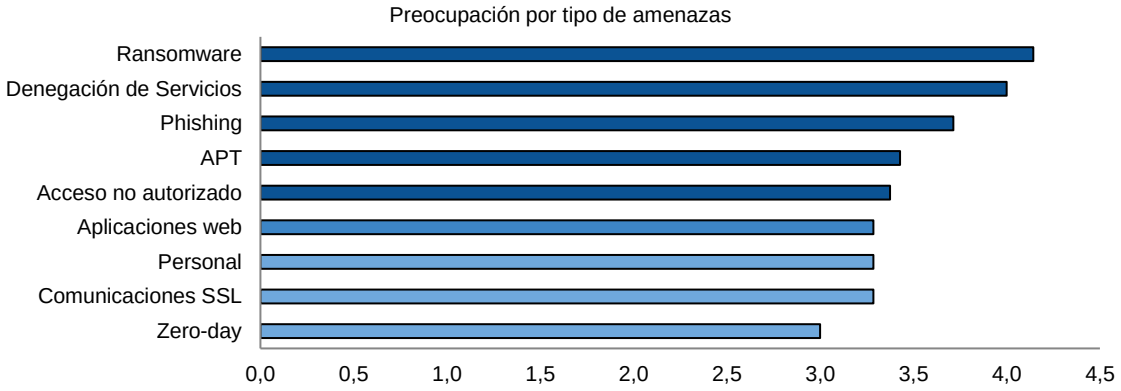
Grafico A2
Situación de Brasil
(En porcentajes)

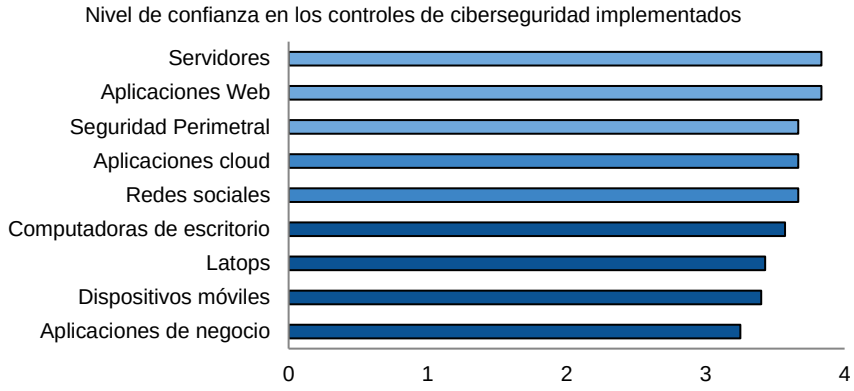


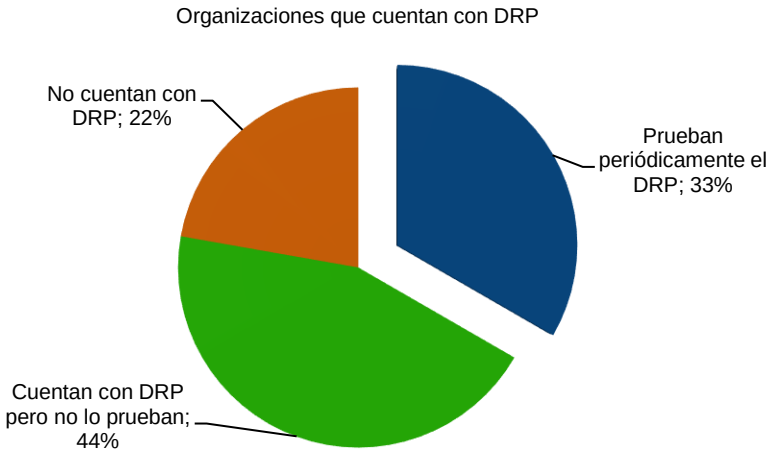

Responsable de seguridad
Otro
11%
CISO
11%
CEO
33%
CIO
45%


Equipos de trabajo
Externo
0%
Interno
44%
Colaboración
Interna /
Externa
56%


Preocupación por objetivo de ataque
Aplicaciones ERP
Datos de clientes
Aplicación logística
Redes de OT
Correo electrónico
Información de empleados
Planes estratégicos
Datos financieros
Propiedad Intelectual
Contratos y facturación
-0,25
0,75
1,75
2,75
3,75


Preocupación por tipo de amenazas
Ransomware
Denegación de Servicios
Phishing
APT
Acceso no autorizado
Aplicaciones web
Personal
Comunicaciones SSL
Zero-day
0,0
0,5
1,0
1,5
2,0
2,5
3,0
3,5
4,0
4,5



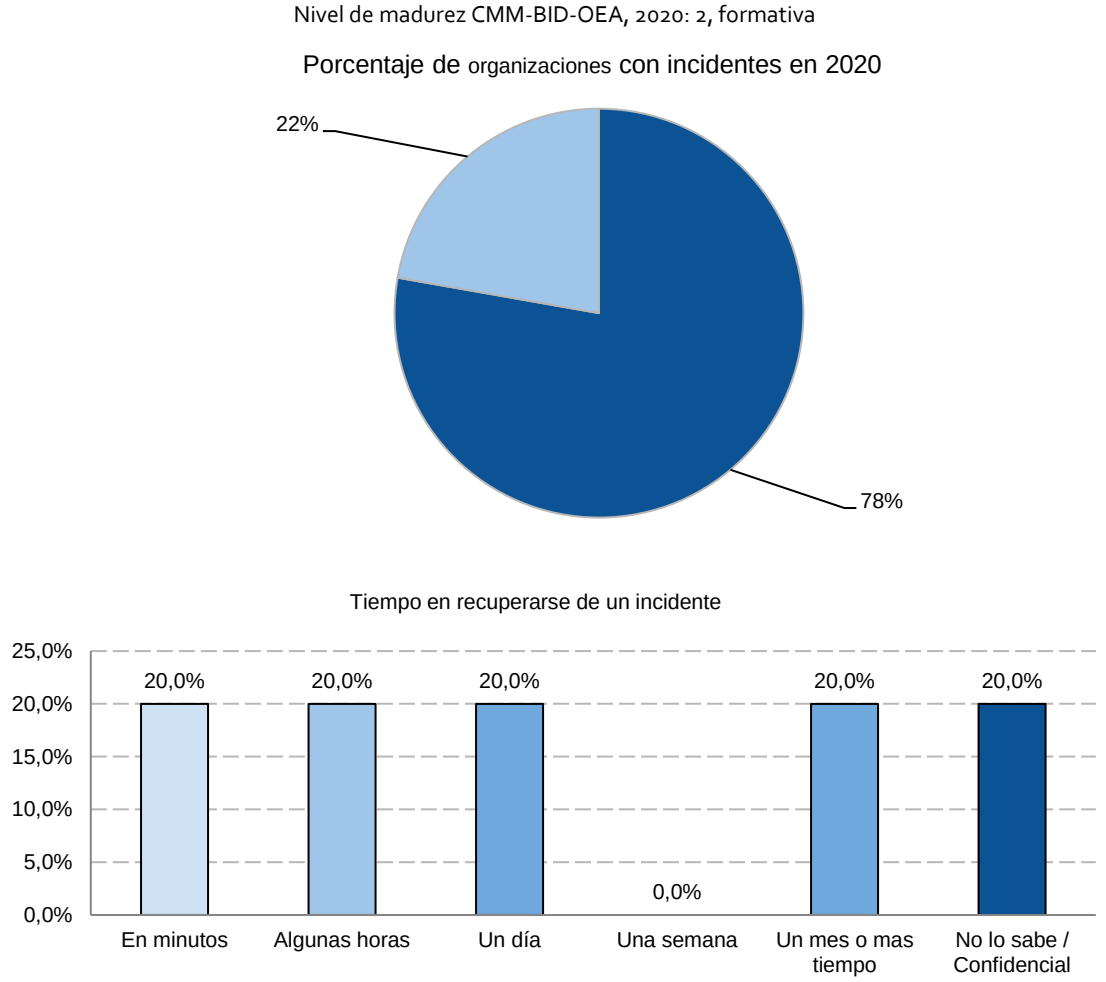


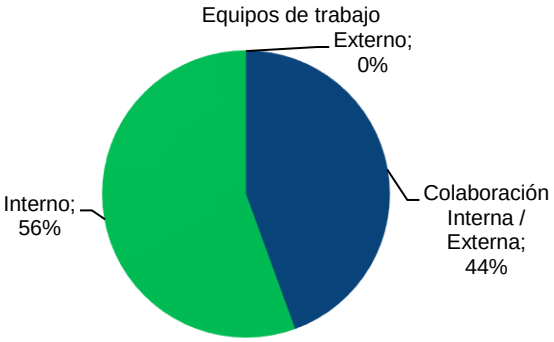
Fuente: Elaboración basada en información obtenida a través de la encuesta aplicada por CEPAL.

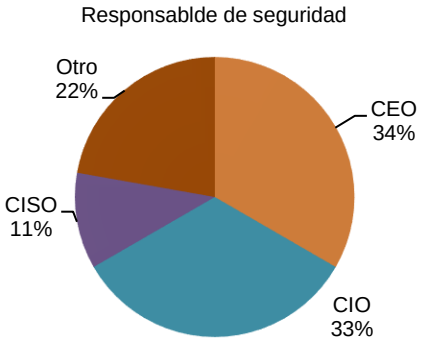
Anexo 3
Situación por país: Chile

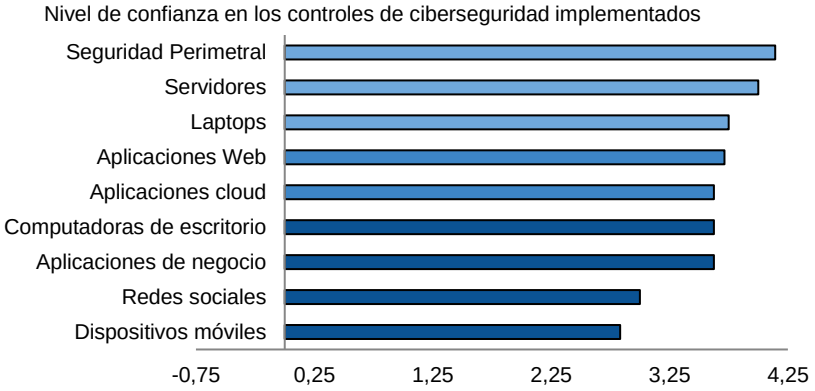
En el caso de Chile puede verificarse una gran evolución en todos sus indicadores, resaltando Estrategia y Respuesta a Incidentes y adicionalmente la evolución en cibercultura.

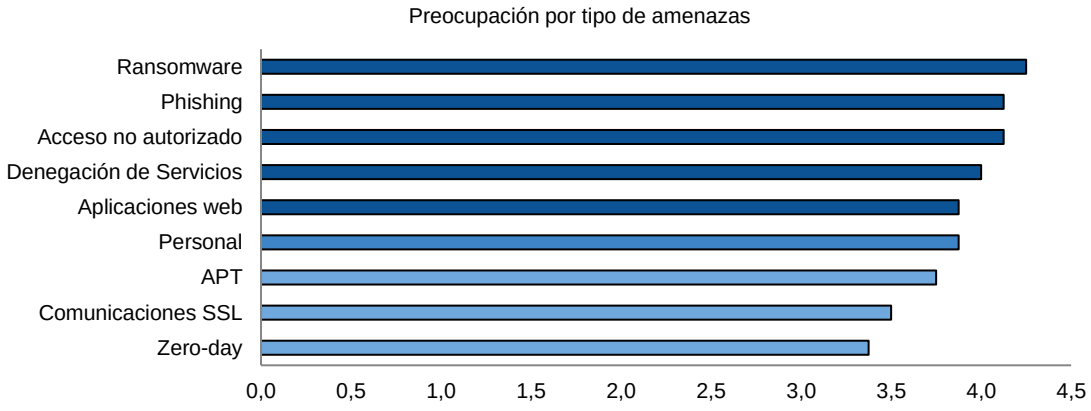
Grafico A3
Situación de Chile
(En porcentajes)

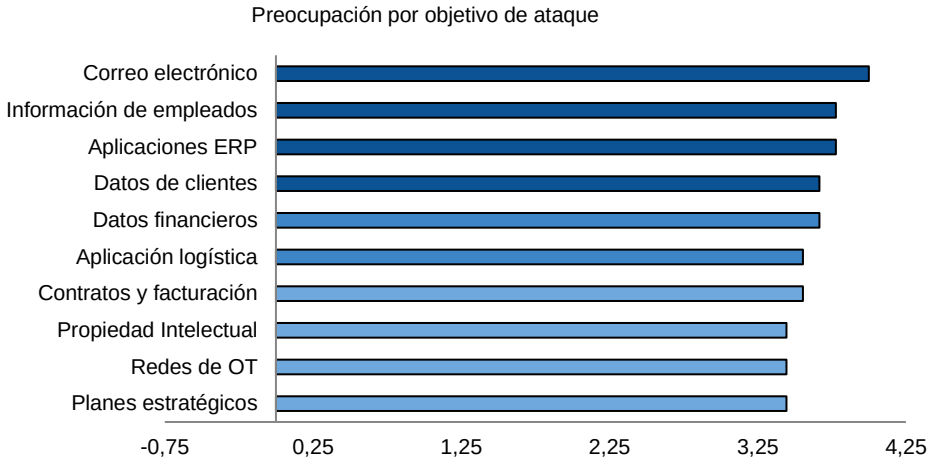



Equipos de trabajo
Externo; 0%
Colaboración Interna / Externa; 44%
Interno; 56%


Responsablde de seguridad
Otro 22%
CEO 34%
CISO 11%
CIO 33%


Nivel de confianza en los controles de ciberseguridad implementados
Seguridad Perimetral
Servidores
Laptops
Aplicaciones Web
Aplicaciones cloud
Computadoras de escritorio
Aplicaciones de negocio
Redes sociales
Dispositivos móviles
-0,75
0,25
1,25
2,25
3,25
4,25


Preocupación por tipo de amenazas
Ransomware
Phishing
Acceso no autorizado
Denegación de Servicios
Aplicaciones web
Personal
APT
Comunicaciones SSL
Zero-day
0,0
0,5
1,0
1,5
2,0
2,5
3,0
3,5
4,0
4,5

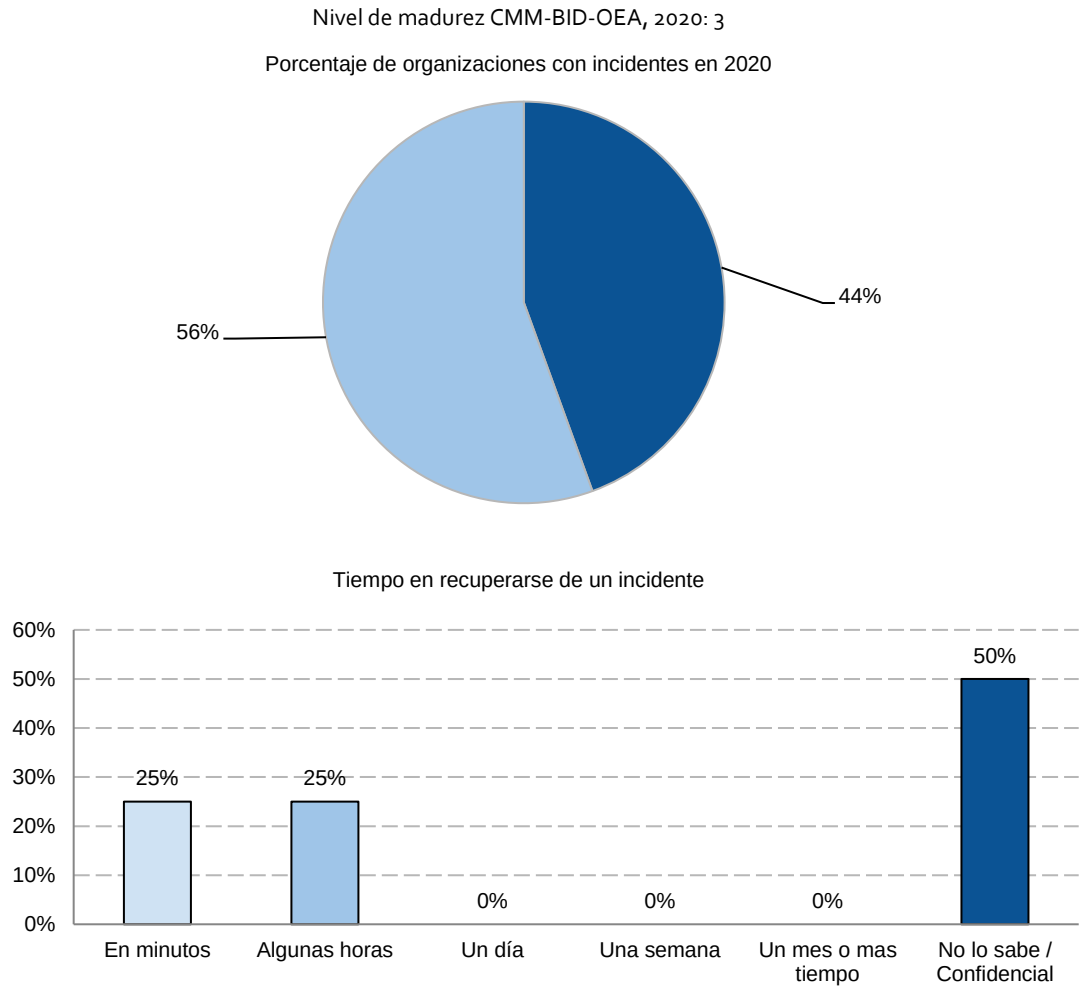


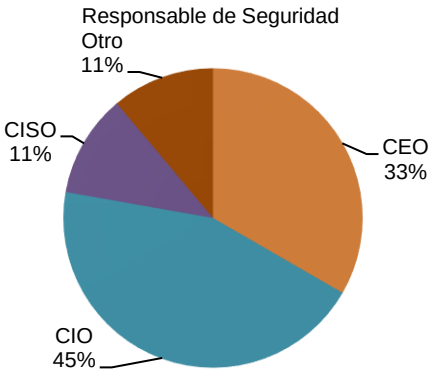
Fuente: Elaboración basada en información obtenida a través de la encuesta aplicada por CEPAL.

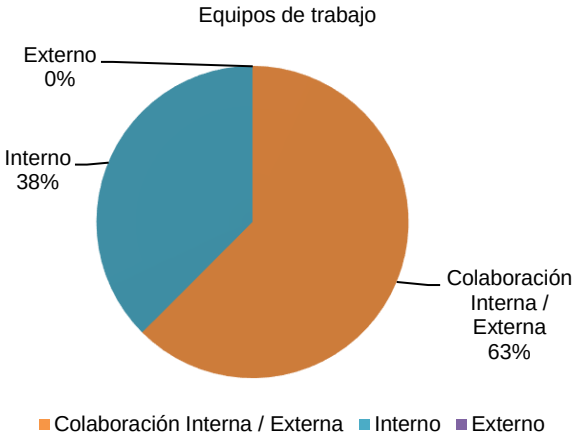
Anexo 4
Situación por país: Colombia

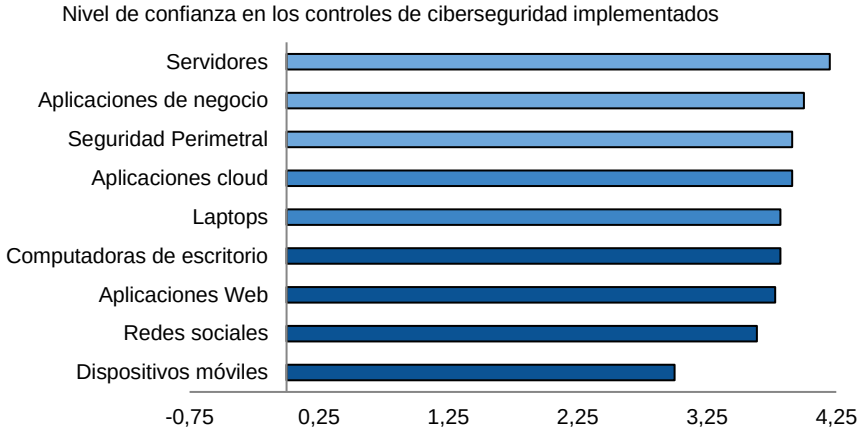
En este caso se encuentra gran evolución en indicadores en los últimos años llegando a un estado de madurez consecuencia de una fuerte política estratégica nacional, que ha impactado positivamente en las organizaciones. El desafío para Colombia es continuar con los esfuerzos para llegar a la concientización individual de la población ajena al ámbito de las organizaciones.

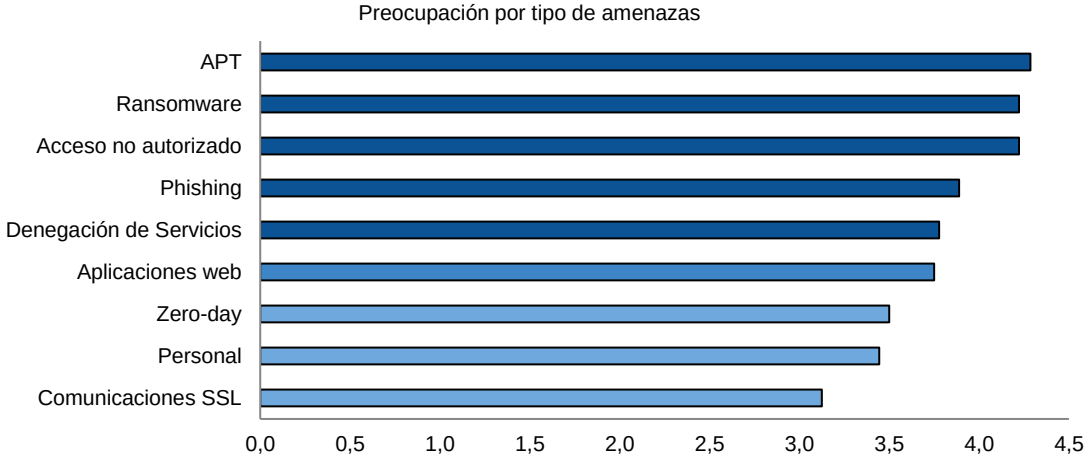
Grafico A4
Situación en Colombia
(En porcentajes)

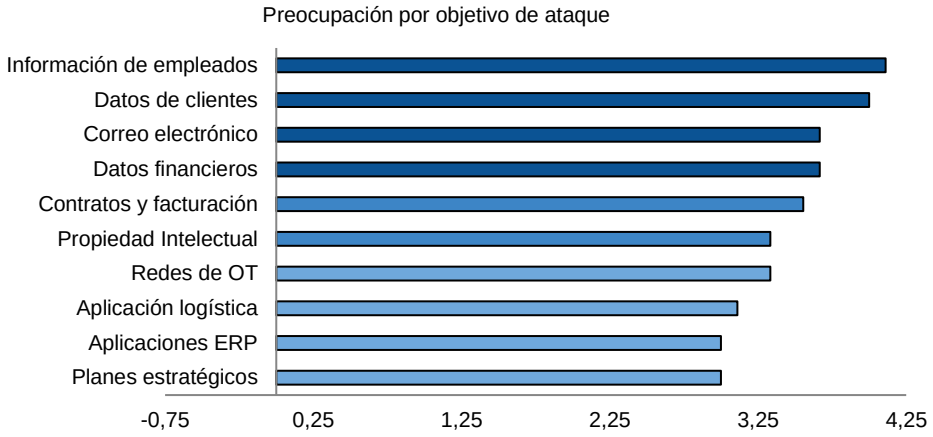


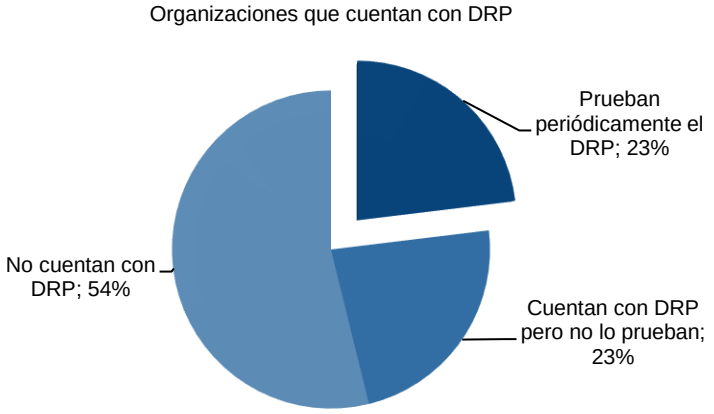

Responsable de Seguridad
Otro
11%
CISO
11%
CEO
33%
CIO
45%


Equipos de trabajo
Externo
0%
Interno
38%
Colaboración
Interna /
Externa
63%
Colaboración Interna / Externa
Interno
Externo


Nivel de confianza en los controles de ciberseguridad implementados
Servidores
Aplicaciones de negocio
Seguridad Perimetral
Aplicaciones cloud
Laptops
Computadoras de escritorio
Aplicaciones Web
Redes sociales
Dispositivos móviles
-0,75
0,25
1,25
2,25
3,25
4,25


Preocupación por tipo de amenazas
APT
Ransomware
Acceso no autorizado
Phishing
Denegación de Servicios
Aplicaciones web
Zero-day
Personal
Comunicaciones SSL
0,0
0,5
1,0
1,5
2,0
2,5
3,0
3,5
4,0
4,5



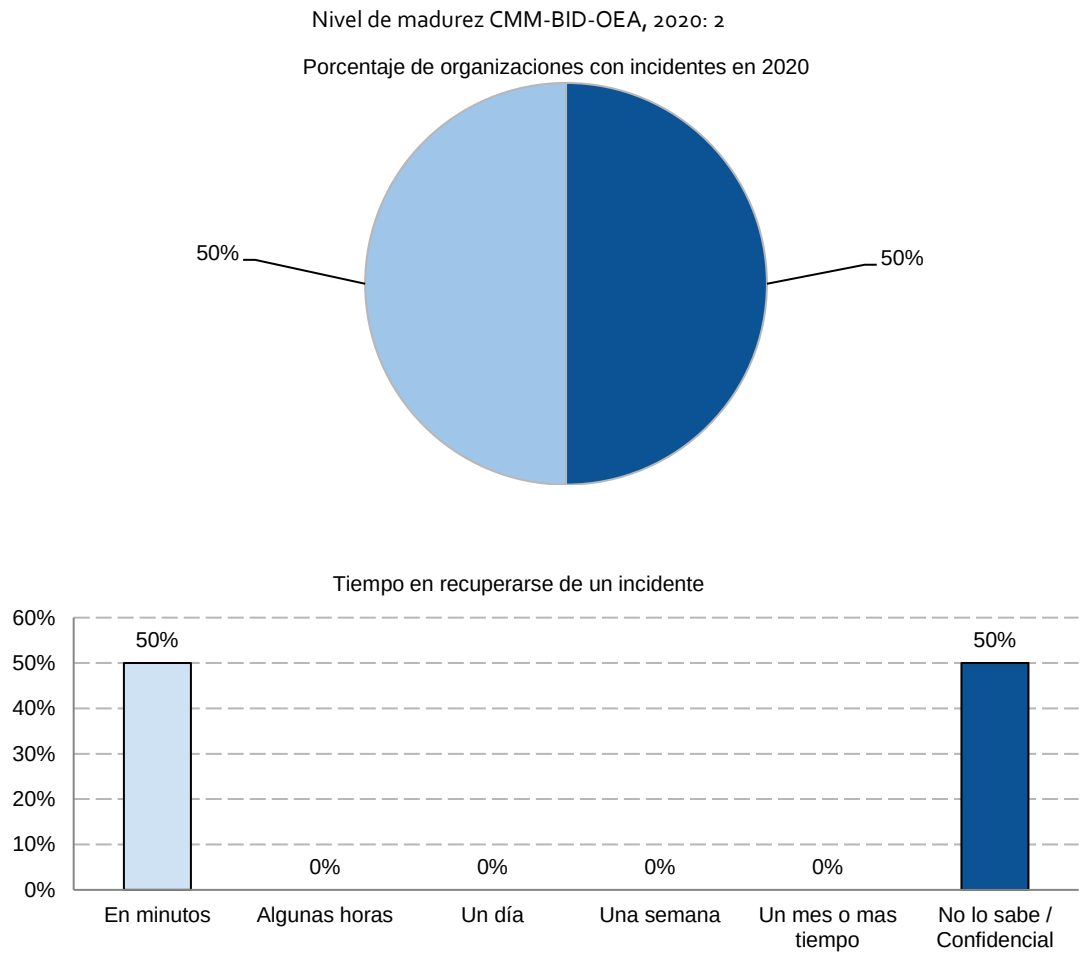


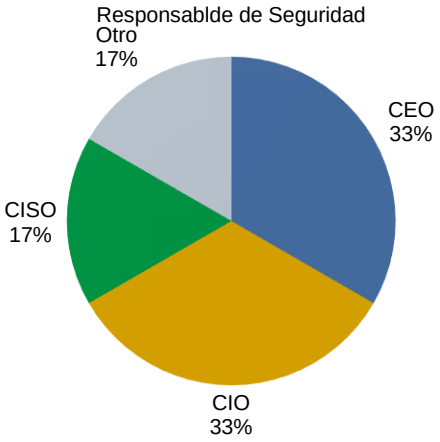
Fuente: Elaboración basada en información obtenida a través de la encuesta aplicada por CEPAL

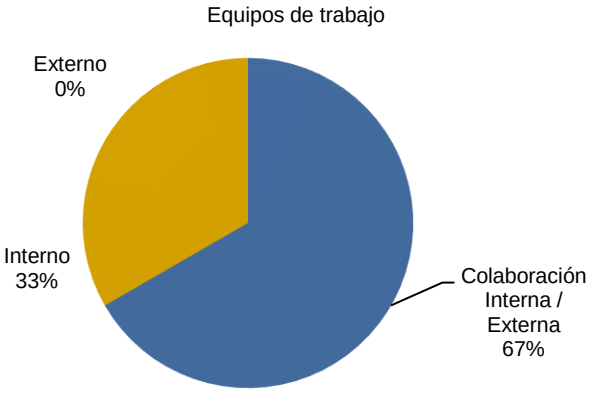
Anexo 5
Situación por país: Ecuador

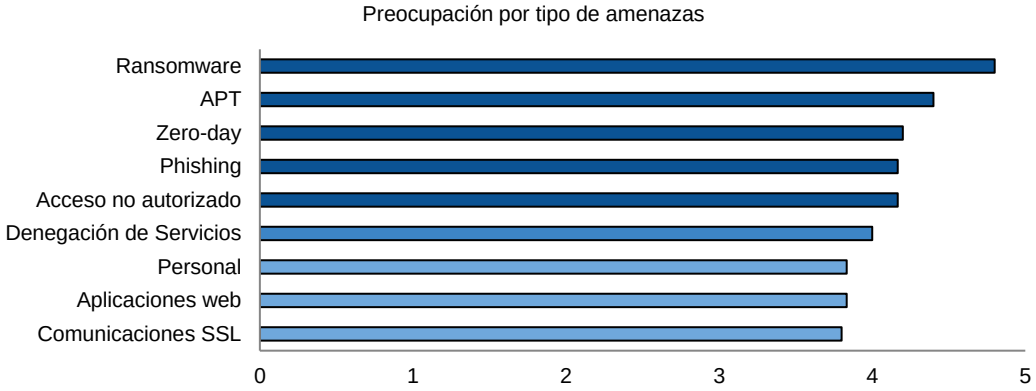
Si bien Ecuador presenta una situación promedio que lo sitúa en fase 2 - Formativa, esto es debido a la definición de un marco legal y estándares que se han creado, en su mayoría en los últimos 4 años, junto a recientes e incipientes avances en cibercultura, permaneciendo los aspectos operativos aún en fase inicial. Ecuador podría encontrar en el desarrollo de estrategias operativas de ciberseguridad a nivel nacional, la catalización de los esfuerzos ya realizados en marco legal y estándares, y de esta manera, avanzar hacia la consolidación de dichos esfuerzos.

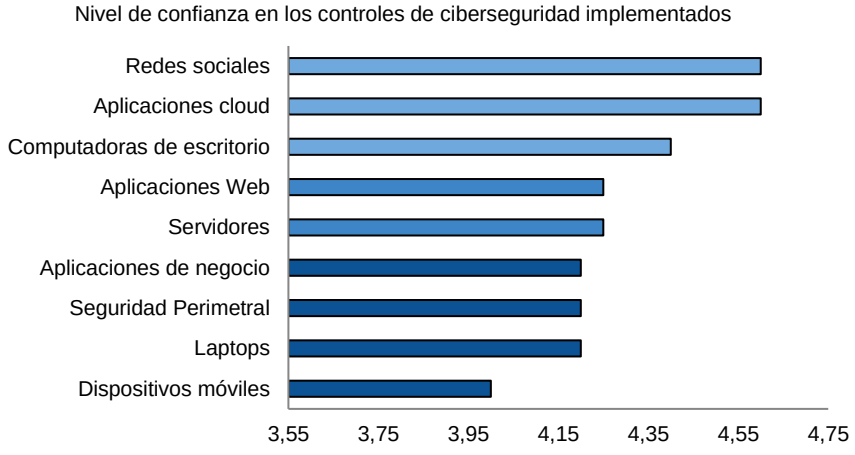
Grafico A5
Situación de Ecuador
(En porcentajes)

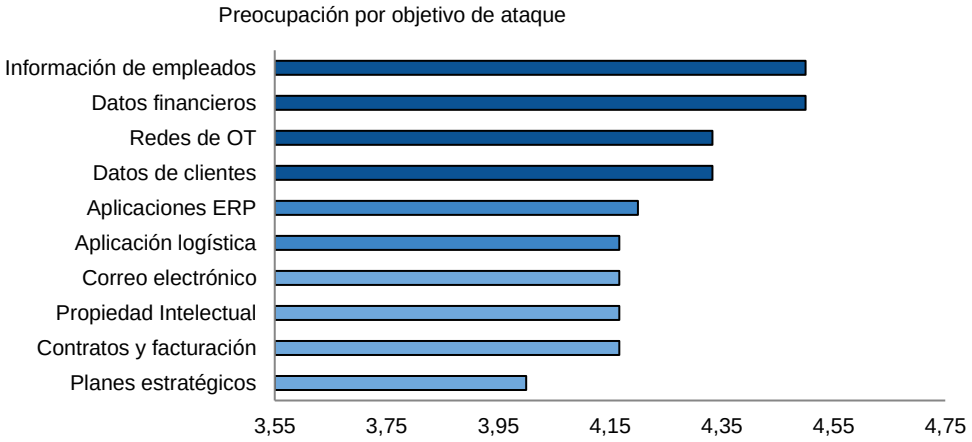



Responsablde de Seguridad
Otro
17%
CEO
33%
CISO
17%
CIO
33%


Equipos de trabajo
Externo
0%
Interno
33%
Colaboración
Interna /
Externa
67%


Preocupación por tipo de amenazas
Ransomware
APT
Zero-day
Phishing
Acceso no autorizado
Denegación de Servicios
Personal
Aplicaciones web
Comunicaciones SSL
0
1
2
3
4
5


Nivel de confianza en los controles de ciberseguridad implementados
Redes sociales
Aplicaciones cloud
Computadoras de escritorio
Aplicaciones Web
Servidores
Aplicaciones de negocio
Seguridad Perimetral
Laptops
Dispositivos móviles
3,55
3,75
3,95
4,15
4,35
4,55
4,75



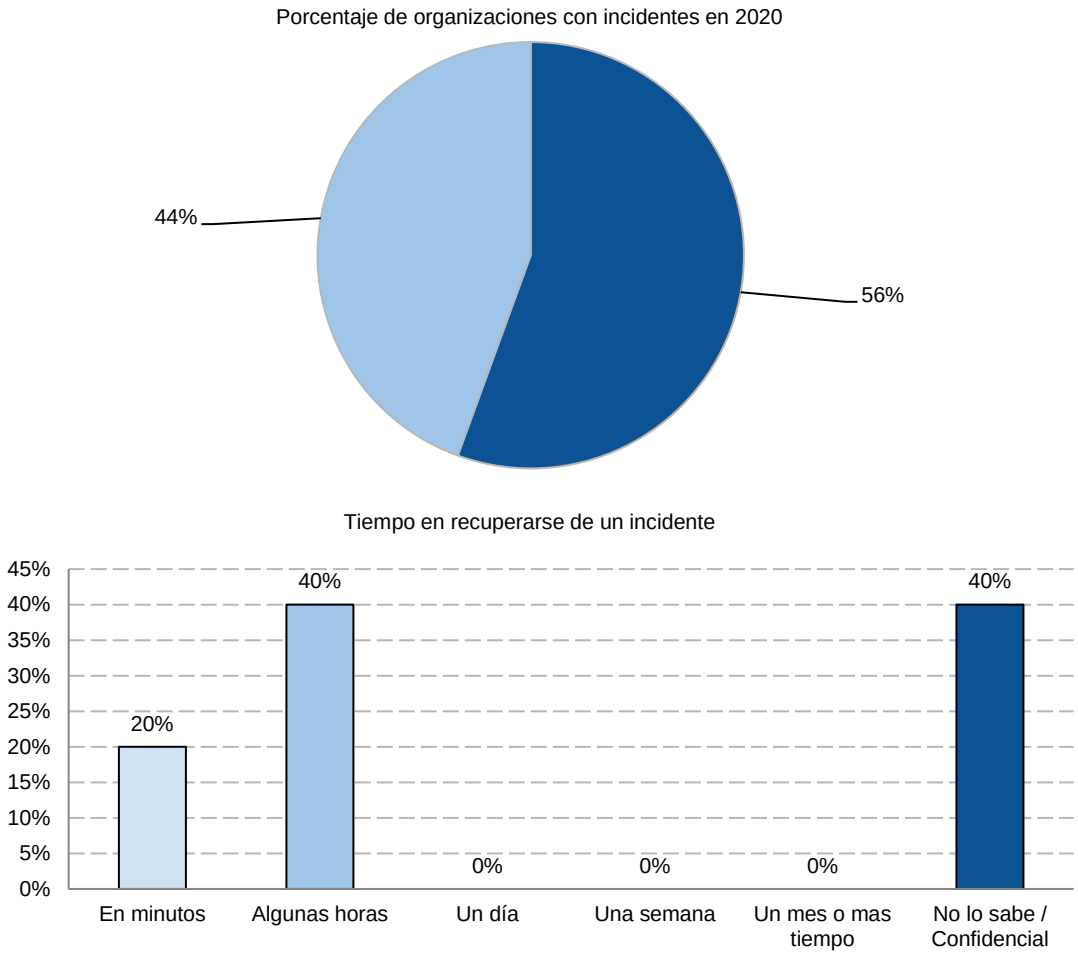
Fuente: Elaboración basada en información obtenida a través de la encuesta aplicada por CEPAL.

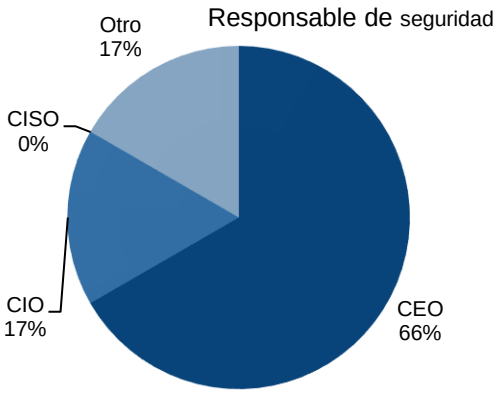
Anexo 6
Situación por país: México

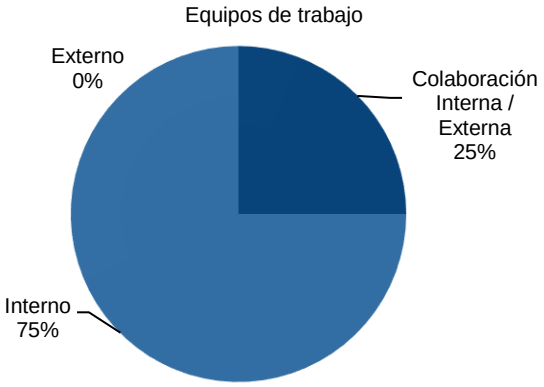
En el caso de México, similar a la situación de Colombia, se encuentra gran evolución en los indicadores de los últimos años, llegando a este estado impulsado por una fuerte política estratégica nacional, que ha impactado positivamente en las organizaciones. Sería natural que continúen en evolución los indicadores de madurez de concientización individual de la población ajena al ámbito de las organizaciones.

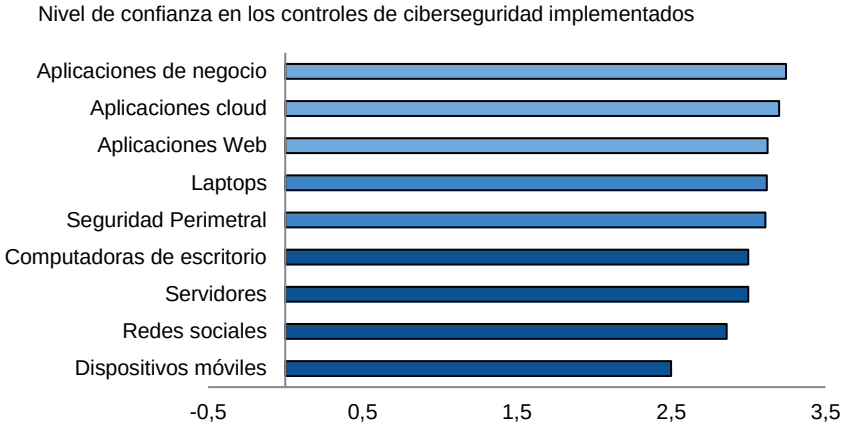
Grafico A6
Situación de México
(En porcentajes)

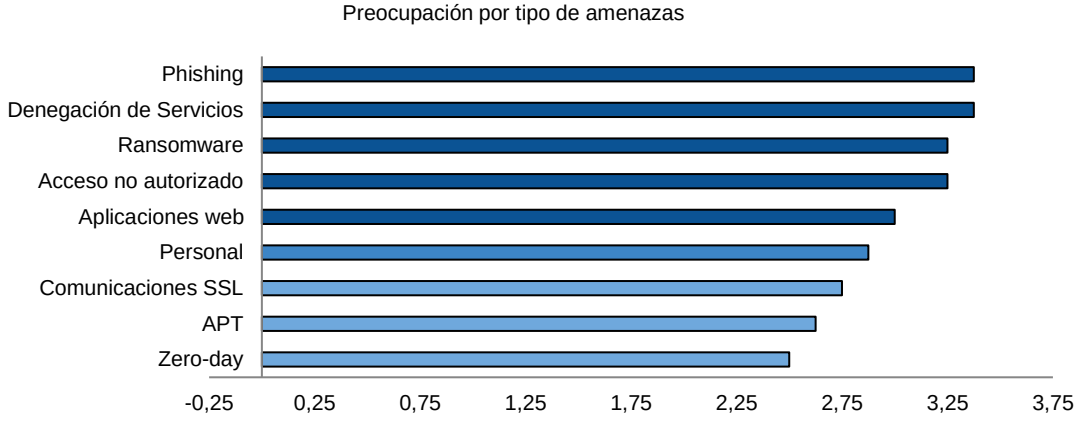
Nivel de madurez CMM-BID-OEA, 2020: 3

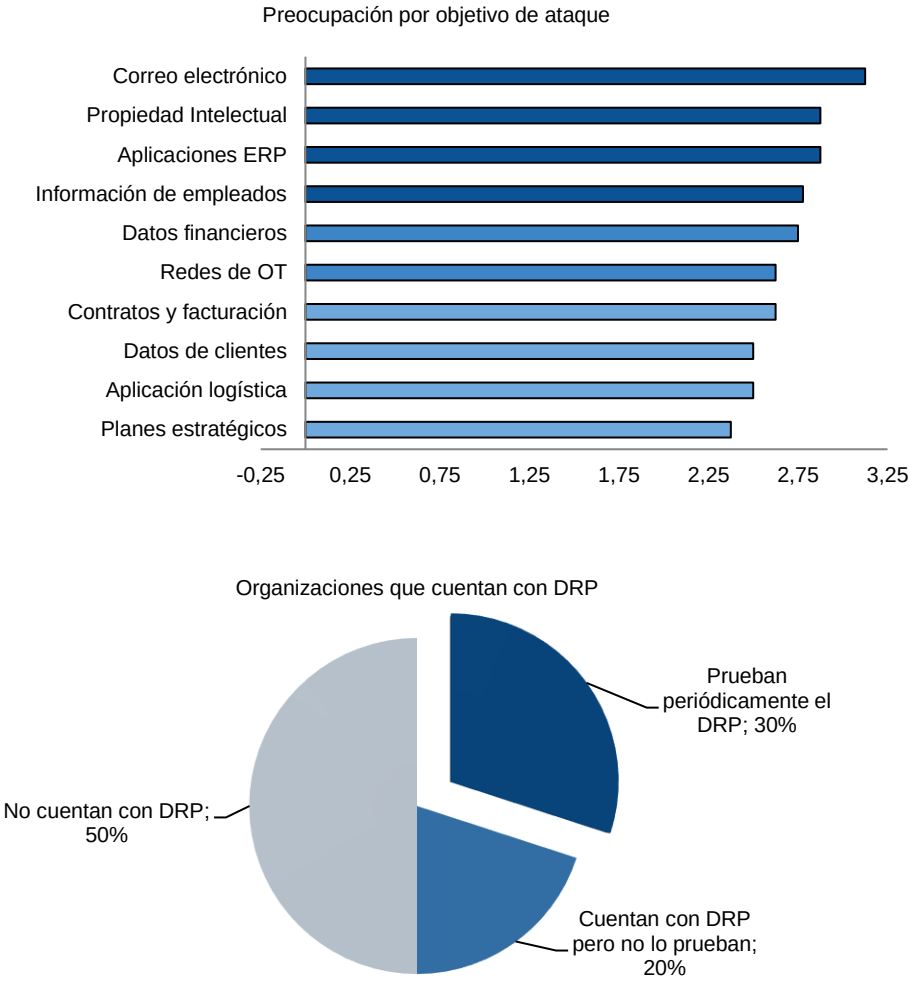



Responsable de seguridad
Otro 17%
CISO 0%
CIO 17%
CEO 66%


Equipos de trabajo
Externo 0%
Colaboración Interna / Externa 25%
Interno 75%


Nivel de confianza en los controles de ciberseguridad implementados
Aplicaciones de negocio
Aplicaciones cloud
Aplicaciones Web
Laptops
Seguridad Perimetral
Computadoras de escritorio
Servidores
Redes sociales
Dispositivos móviles
-0,5
0,5
1,5
2,5
3,5


Preocupación por tipo de amenazas
Phishing
Denegación de Servicios
Ransomware
Acceso no autorizado
Aplicaciones web
Personal
Comunicaciones SSL
APT
Zero-day
-0,25
0,25
0,75
1,25
1,75
2,25
2,75
3,25
3,75

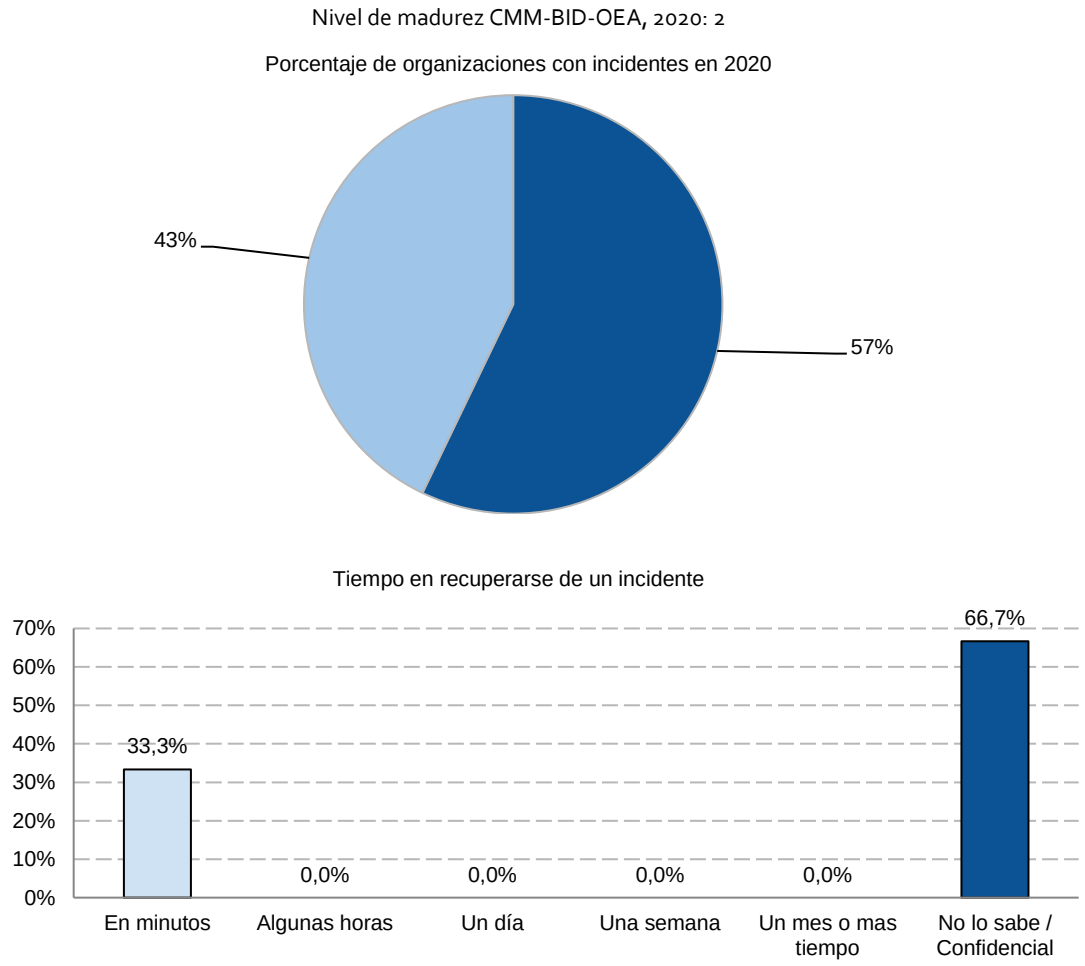


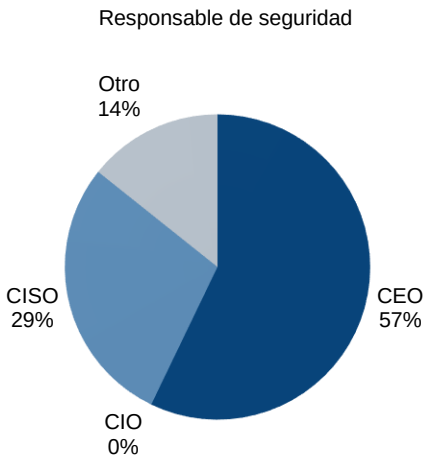
Fuente: Elaboración basada en información obtenida a través de la encuesta aplicada por CEPAL.

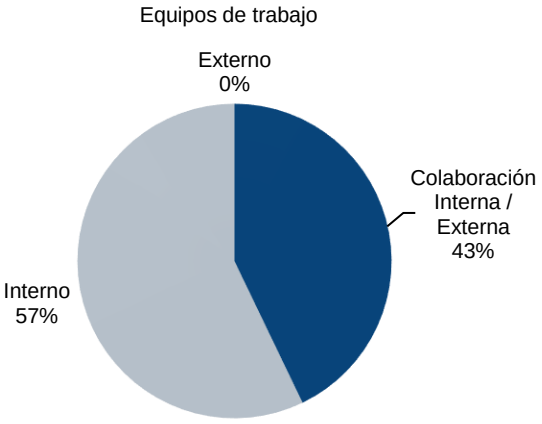
Anexo 7
Situación por país: Panamá

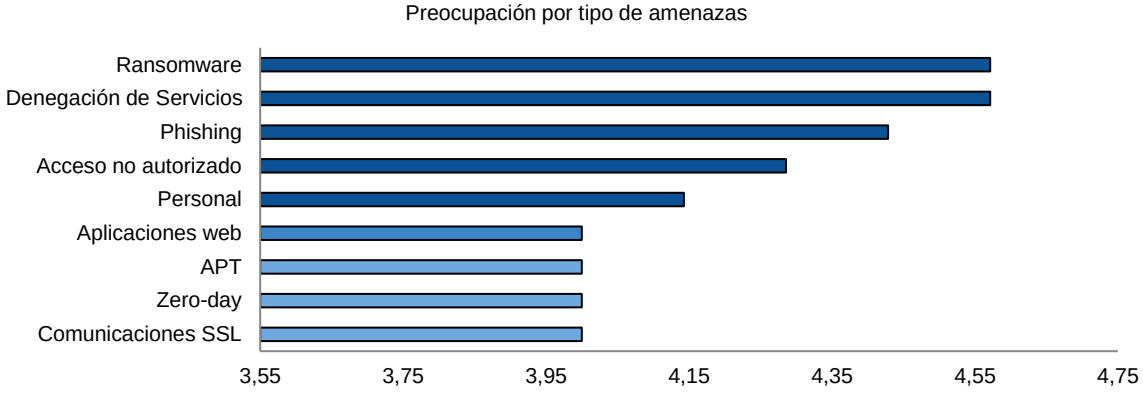
Se observa en Panamá una continuidad en los indicadores de CMM entre los años 2016 y 2020 (BID y OEA, 2020), situación que combinada con el interés que su estructura financiera despierta en la ciberdelincuencia, podría indicar la necesidad de una mejora tanto en lo concerniente a infraestructura como en el aspecto cultural.

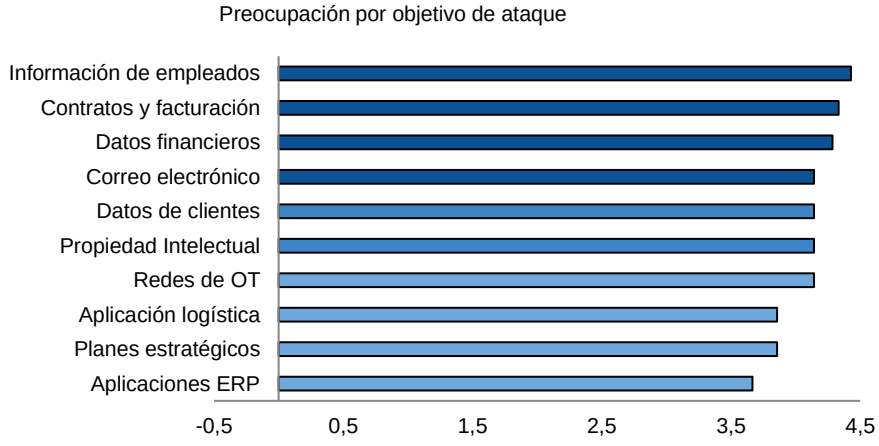
Grafico A7
Situación de Panamá
(En porcentajes)

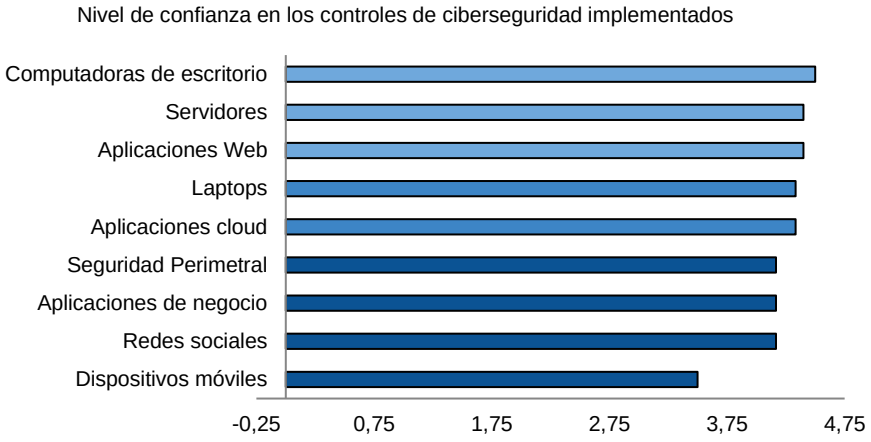



Responsable de seguridad
Otro
14%
CISO
29%
CEO
57%
CIO
0%


Equipos de trabajo
Externo
0%
Colaboración
Interna /
Externa
43%
Interno
57%


Preocupación por tipo de amenazas
Ransomware
Denegación de Servicios
Phishing
Acceso no autorizado
Personal
Aplicaciones web
APT
Zero-day
Comunicaciones SSL
3,55
3,75
3,95
4,15
4,35
4,55
4,75


Preocupación por objetivo de ataque
Información de empleados
Contratos y facturación
Datos financieros
Correo electrónico
Datos de clientes
Propiedad Intelectual
Redes de OT
Aplicación logística
Planes estratégicos
Aplicaciones ERP
-0,5
0,5
1,5
2,5
3,5
4,5

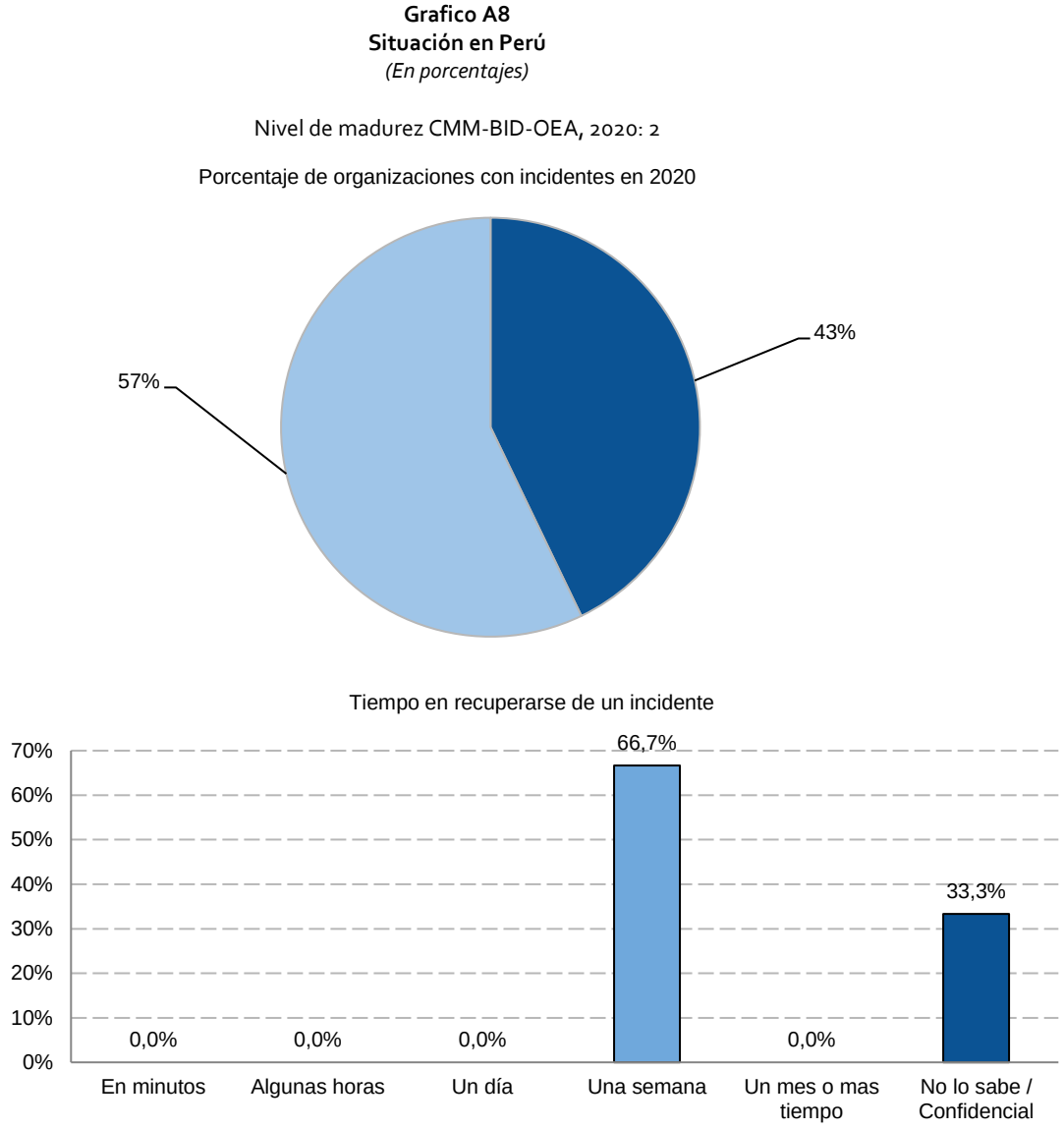


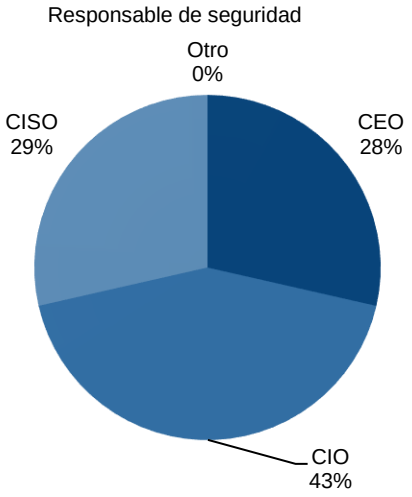
Fuente: Elaboración basada en información obtenida a través de la encuesta aplicada por CEPAL.

Anexo 8
Situación por país: Perú

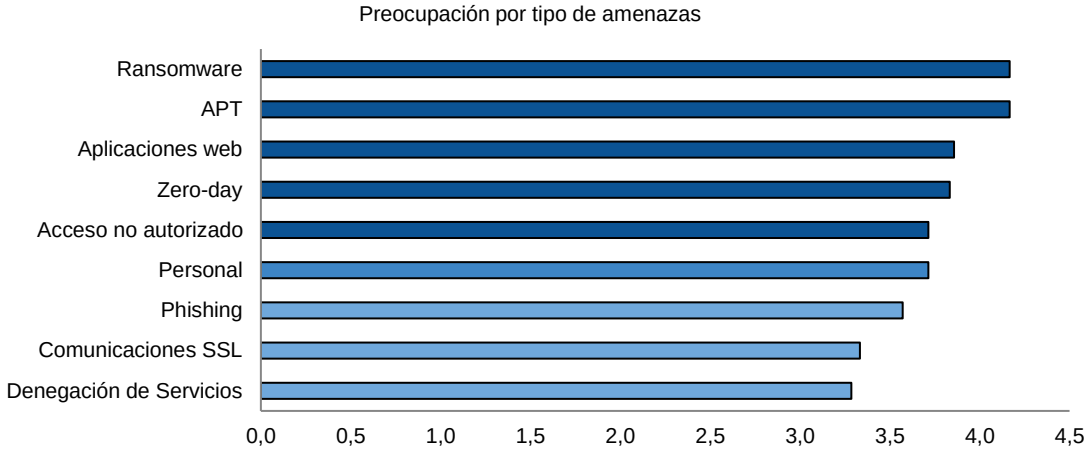
Perú presenta gran evolución en indicadores en los últimos años llegando a un estado de madurez en etapa 2 como consecuencia de una fuerte política estratégica nacional, que ha impactado positivamente en las organizaciones. Como el caso de Colombia y México, se debería continuar con los esfuerzos para llegar a la concientización individual de la población ajena al ámbito de las organizaciones.

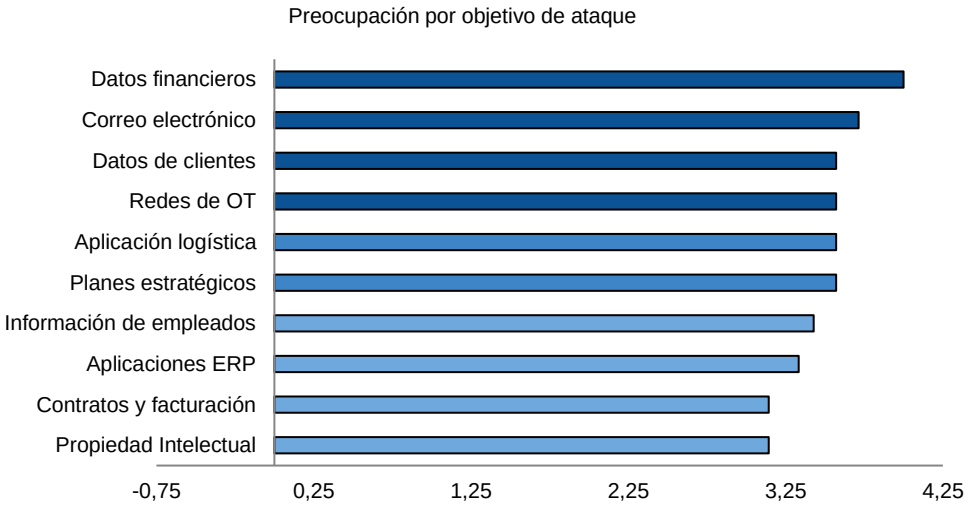
Grafico A8
Situación en Perú
(En porcentajes)

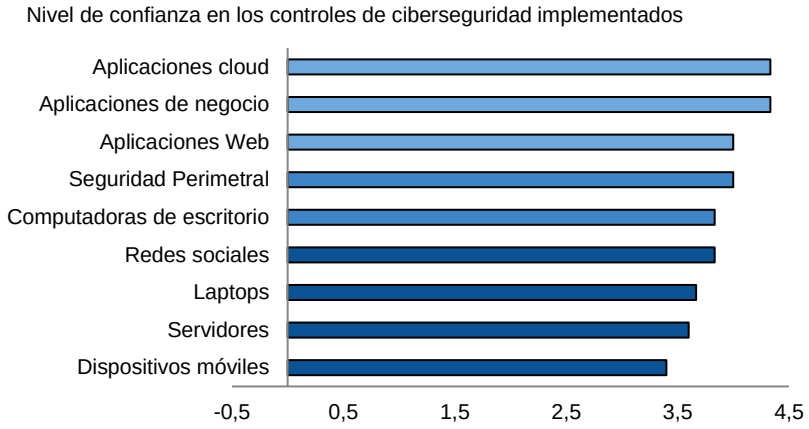


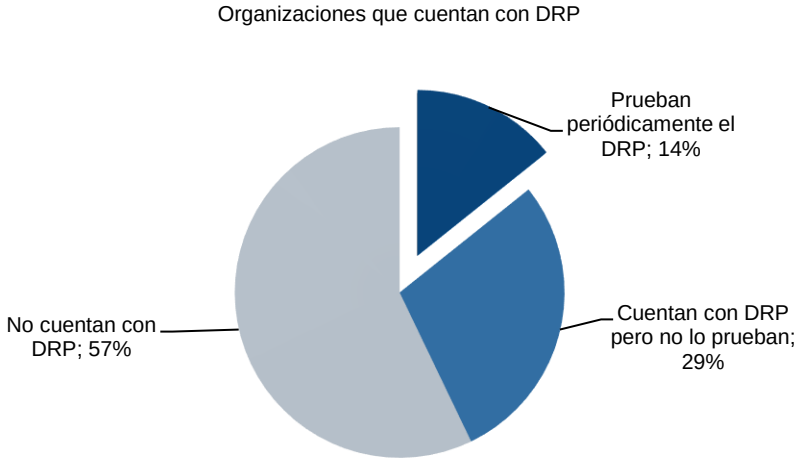

Responsable de seguridad
Otro
0%
CISO
29%
CEO
28%
CIO
43%


Equipos de trabajo
Externo
0%
Interno
14%
Colaboración
Interna /
Externa
86%


Preocupación por tipo de amenazas
Ransomware
APT
Aplicaciones web
Zero-day
Acceso no autorizado
Personal
Phishing
Comunicaciones SSL
Denegación de Servicios
0,0
0,5
1,0
1,5
2,0
2,5
3,0
3,5
4,0
4,5


Preocupación por objetivo de ataque
Datos financieros
Correo electrónico
Datos de clientes
Redes de OT
Aplicación logística
Planes estratégicos
Información de empleados
Aplicaciones ERP
Contratos y facturación
Propiedad Intelectual
-0,75
0,25
1,25
2,25
3,25
4,25



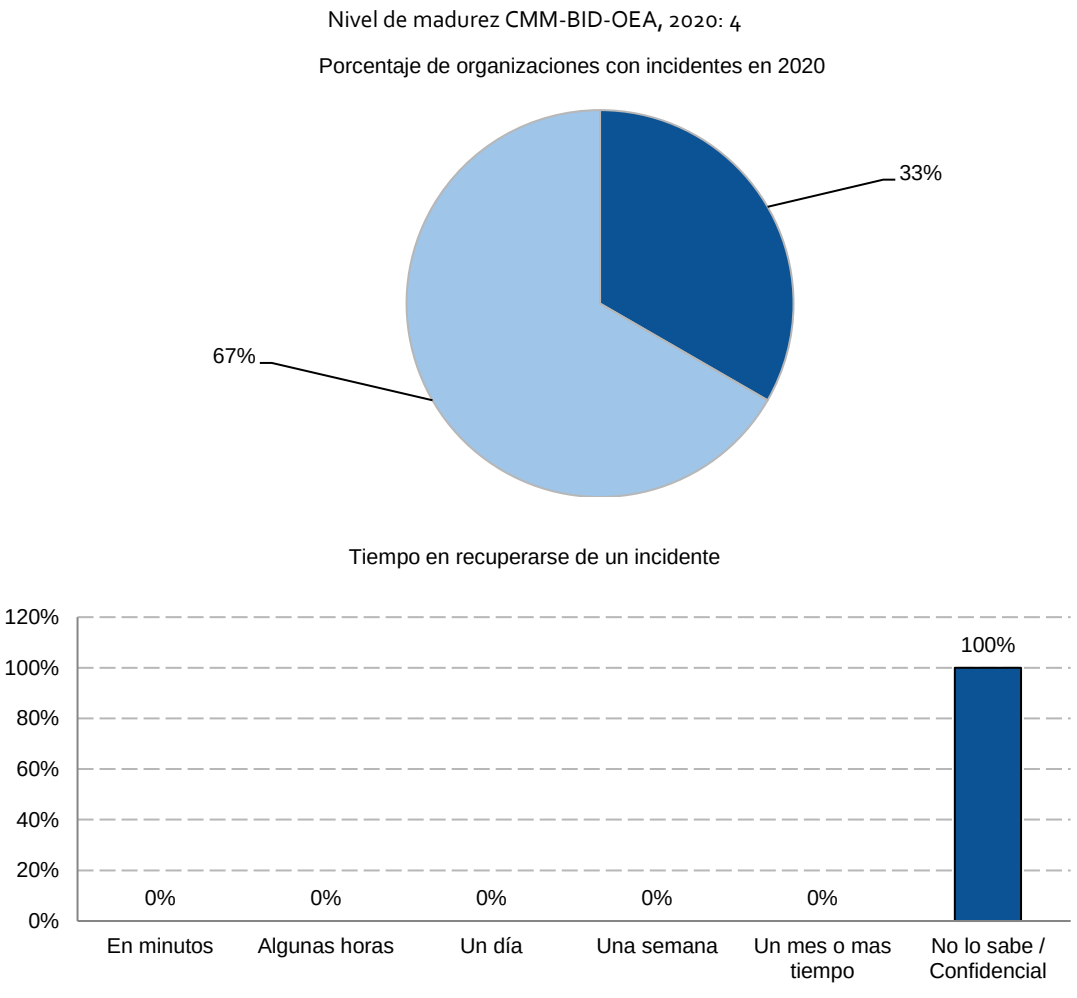


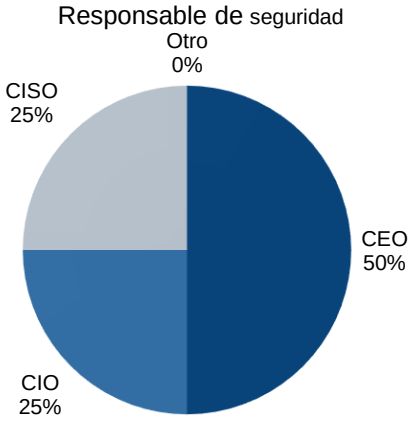
Fuente: Elaboración basada en información obtenida a través de la encuesta aplicada por CEPAL.

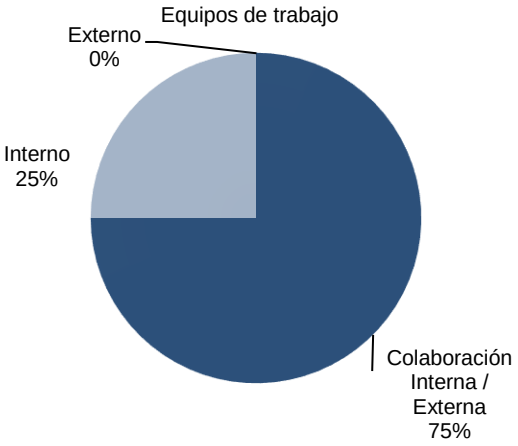
Anexo 9
Situación por país: Uruguay

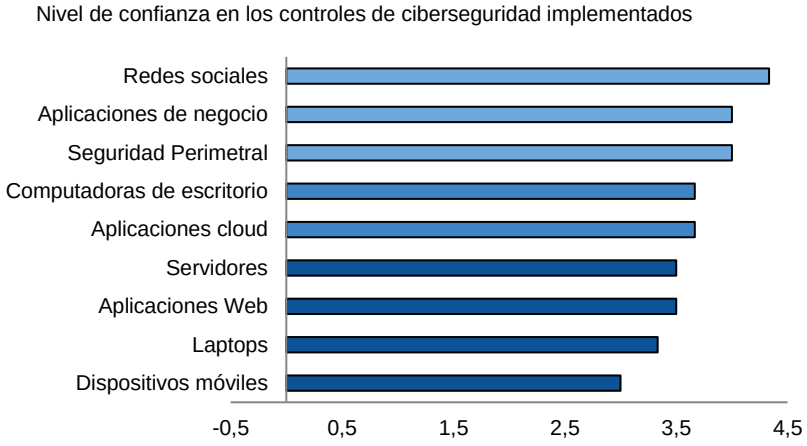
Se observa en Uruguay desde 2016 una estrategia clara de ciberseguridad nacional con consistente evolución en 2020 (BID y OEA, 2020) llegando en este año a la etapa estratégica del modelo de CMM. Se destaca la gestión de respuesta a incidentes en etapa dinámica y el mismo nivel de madurez en protección de datos personales, ambos relacionados con un elevado nivel de concientización del estado nacional en ciberseguridad.

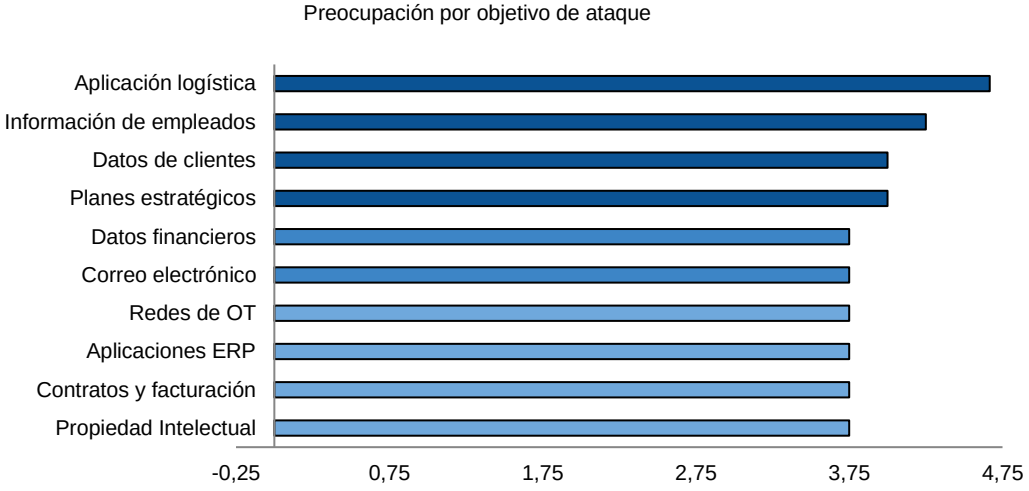
Grafico A9
Situación en Uruguay
(En porcentajes)

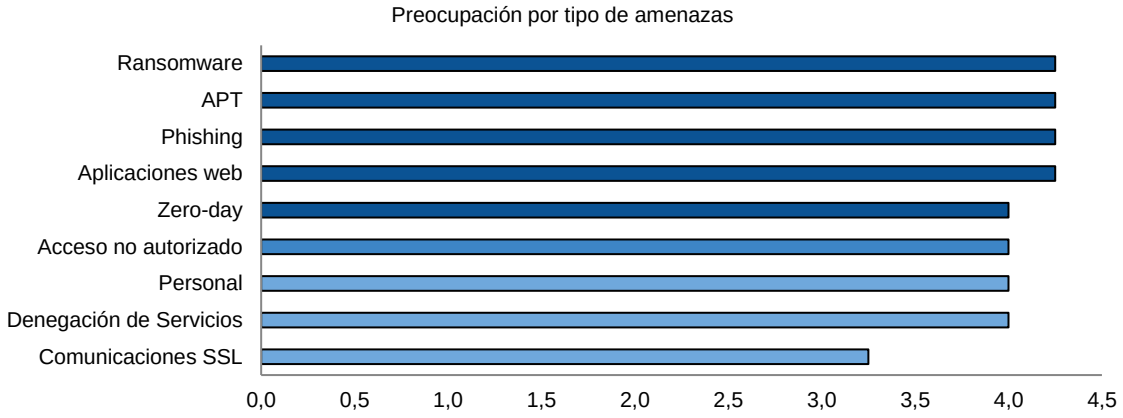



Responsable de seguridad
Otro
0%
CISO
25%
CEO
50%
CIO
25%


Equipos de trabajo
Externo
0%
Interno
25%
Colaboración
Interna /
Externa
75%


Nivel de confianza en los controles de ciberseguridad implementados
Redes sociales
Aplicaciones de negocio
Seguridad Perimetral
Computadoras de escritorio
Aplicaciones cloud
Servidores
Aplicaciones Web
Laptops
Dispositivos móviles
-0,5
0,5
1,5
2,5
3,5
4,5


Preocupación por objetivo de ataque
Aplicación logística
Información de empleados
Datos de clientes
Planes estratégicos
Datos financieros
Correo electrónico
Redes de OT
Aplicaciones ERP
Contratos y facturación
Propiedad Intelectual
-0,25
0,75
1,75
2,75
3,75
4,75



Fuente: Elaboración basada en información obtenida a través de la encuesta aplicada por CEPAL.

NACIONES UNIDAS

CEPAL

Serie

Desarrollo Productivo

Números publicados

Un listado completo así como los archivos pdf están disponibles en www.cepal.org/publicaciones

228. Estado de la ciberseguridad en la logística de América Latina y el Caribe, Rodrigo Díaz (LC/TS.2021/108), 2021.
227. Mesoamérica digital 2025: propuesta para una agenda digital mesoamericana, Juan Jung (LC/TS.2021/77), 2021.
226. Infraestructura de Internet en América Latina: puntos de intercambio de tráfico, redes de distribución de contenido, cables submarinos y centros de datos, Raúl Echeberría (LC/TS.2020/120), 2020.
225. Cybersecurity and the role of the Board of Directors in Latin America and the Caribbean, Héctor J. Lehuedé, (LC/TS.2020/103), 2020.
224. Institutional change and political conflict in a structuralist model, Gabriel Porcile y Diego Sanchez-Ancochea (LC/TS.2020/55), 2020.
223. Corporate governance and data protection in Latin America and the Caribbean, Héctor J. Lehuedé (LC/TS.2019/38), 2019.
222. El financiamiento de la bioeconomía en países seleccionados de Europa, Asia y África: experiencias relevantes para América Latina y el Caribe. Adrián G. Rodríguez, Rafael H. Aramendis y Andrés O. Mondaini (LC/TS.2018/101), 2018.
221. The long-run effects of portfolio capital inflow booms in developing countries: permanent structural hangovers after short-term financial euphoria, Alberto Botta (LC/TS.2018/96) 2018.
220. Agencias regulatorias del Estado, aprendizaje y desarrollo de capacidades tecnológicas internas: los casos del Servicio Nacional de Pesca y Acuicultura y el Servicio Nacional de Geología y Minería de Chile, Rodrigo Cáceres, Marco Dini y Jorge Katz (LC/TS.2018/40), 2018.
219. Capital humano para la transformación digital en América Latina, Raúl L. Katz (LC/TS.2018/25), 2018.

DESARROLLO PRODUCTIVO

Números publicados:

228 Estado de la ciberseguridad en la logística de América Latina y el Caribe
Rodrigo Mariano Díaz

227 Mesoamérica digital 2025
Propuesta para una agenda digital mesoamericana
Juan Jung

226 Infraestructura de Internet en América Latina
Puntos de intercambio de tráfico, redes de distribución de contenido, cables submarinos y centros de datos
Raúl Echeberría

225 Cybersecurity and the role of the Board of Directors in Latin America and the Caribbean
Héctor J. Lehuedé

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

LC/TS.2021/108