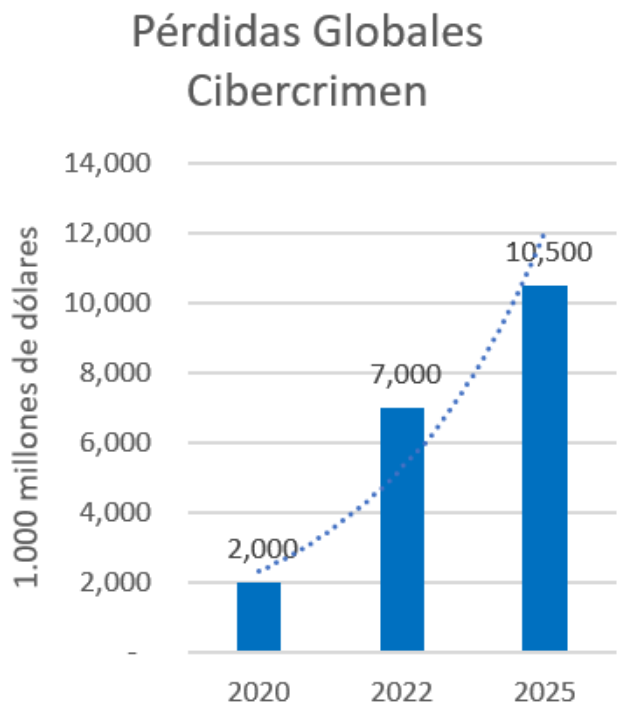
Perspectiva global y regional de la ciberseguridad

Rodrigo Mariano Díaz

Importancia de la Ciberseguridad

1. Salvaguardar la Seguridad Nacional a través de la prevención de ataques a los sistemas y datos de inteligencia y militares.
2. Asegurar la confidencialidad de los datos personales y el cumplimiento normativo y regulatorio vigente.
3. Comprender el papel crucial que desempeña la ciberseguridad en la gobernanza y el riesgo corporativo
4. Proteger la infraestructura crítica en un entorno de creciente dependencia de la tecnología y la conectividad en línea.
5. Preservar a las organizaciones de ataques cibernéticos que pueden provocar pérdidas económicas por discontinuidad operativa, de la propiedad intelectual o de la confianza de sus clientes.

Impacto de los Ciberataques en la Sociedad



Fuente: Secureworks.

https://www.secureworks.com/resources/rp-boardroom-cybersecurity-report

Riesgos –Probabilidad vs Impacto

Fuente: Foro Económico Mundial
http://wef.ch/risks2021

Desarrollos de la CEPAL en Ciberseguridad

05-20	• Seminarios de concientización de ciberseguridad ante la demanda relacionada con el aislamiento declarado con la aparición del coronavirus COVID-19
09-20	• Publicación Desarrollo Productivo - La Ciberseguridad y el rol del Comité Directivo en América Latina y el Caribe
11-20	• Boletín FAL 382 - La ciberseguridad en tiempos del COVID-19 y el tránsito hacia una ciberinmunidad
09-21	• Publicación Desarrollo Productivo - Estado de la ciberseguridad en la logística de América Latina y el Caribe
08-22	• Documento de Proyecto - Ciberseguridad en cadenas de suministros inteligentes en América Latina y el Caribe
08-23	• Publicación Desarrollo Productivo - Ciberataques en logística e infraestructura crítica en América Latina y el Caribe

Estado de la ciberseguridad en la logística de América Latina y el Caribe (ALC) Resultados clave:

Un diagnóstico de los acontecimientos relacionados con la ciberseguridad, ocurridos en los últimos años y especialmente durante el brote de COVID-19 en la región.

Se encontró que, en ALC 7 de cada 10 empresas recibieron al menos un ataque en el año 2020.

En ALC, la problemática de ciberseguridad alcanza niveles intermedios e insuficientes para las expectativas de desarrollo tecnológico estratégico.

Se destaca la existencia de los *Computer Security Incident Response Team* (CSIRT) y la necesidad de reforzar la colaboración regional.

Si bien las PyMes reciben los ataques, no cuentan con los recursos humanos y económicos suficientes para abordar los desafíos de ciberseguridad y pueden afectar a la cadena completa.

Estado de la ciberseguridad en la logística de América Latina y el Caribe (ALC)

Lineamientos estratégicos:

- Promover desarrollos estratégicos transfronterizos de ciberseguridad desde las instituciones de alcance regional.
- Estimular a los estados a elaborar su Estrategia Nacional de Ciberseguridad basada en la guía publicada por la Unión Internacional de Telecomunicaciones en 2018.
- Desarrollar el capital humano regional hacia una cultura de ciberinmunidad mediante la incorporación de contenidos cognitivos adecuados para cada nivel educativo.
- Fortalecer el marco normativo y regulatorio para elevar el nivel de confianza en ciberseguridad reduciendo el riesgo de inversión regional.

Ciberseguridad en cadenas de suministros inteligentes en América Latina y el Caribe

Resultados clave:

Presentación de un enfoque técnico amplio para cubrir las necesidades y herramientas públicas y privadas necesarias para abordar la ciberinmunidad.

Determinación de las limitaciones que aún existen para combatir el cibercrimen en un escenario de incesante crecimiento de ataques en cantidad y costo promedio.

Inventario de las fortalezas y debilidades de las tecnologías de la Industria 4.0 aplicada a la logística.

Descripción de las organizaciones globales, regionales y nacionales apropiadas para atender los ciberataques.

Pedidos de rescate de información orientados al valor de los datos y el cumplimiento regulatorio.

Ciberseguridad en cadenas de suministros inteligentes en América Latina y el Caribe

Lineamientos estratégicos:

- Cultivar las visiones estratégicas de las Naciones Unidas, la Organización de Estados Americanos y la Unión Europea sobre la problemática de ciberseguridad.
- Sostener el esfuerzo de los organismos internacionales en coordinar acciones y alinear políticas que gobiernen los datos como bienes patrimoniales e inmateriales.
- Continuar en el proceso de transformación digital incorporando la ciberseguridad desde las etapas iniciales de cada proyecto, siguiendo los estándares internacionales recomendados.

Ciberataques en logística e infraestructura crítica en América Latina y el Caribe (ALC)

Objetivos:

- Comprender el papel crucial que desempeña la ciberseguridad en la gobernanza y el riesgo corporativo
- Revisión exhaustiva de los incidentes ocurridos en ALC durante el periodo comprendido entre 2020 y 2022, mediante investigación, informes e información obtenida de los equipos de respuesta a incidentes de seguridad (CSIRT)
- Presentar lineamientos estratégicos con el objetivo de elevar los niveles de protección cibernética de la región

Ciberataques en logística e infraestructura crítica en América Latina y el Caribe (ALC)

Resultados clave:

- El abordaje permanente a la problemática ha logrado instaurar la idea de que la ciberseguridad representa un riesgo mayor y que su desatención puede erosionar la confianza y reputación de las organizaciones en la región.
- Se han logrado algunos avances en normativas de protección de datos y ciberseguridad, aunque no todos los países de ALC cuentan con marcos regulatorios, generando diferencias significativas en la región.
- Importante crecimiento en severidad y cantidad de los incidentes que han afectado a las cadenas logísticas y a la infraestructura crítica, información recolectada de los CSIRT.
- 9 de cada 10 organizaciones recibieron un ataque en 2022.

Ciberataques en logística e infraestructura crítica en América Latina y el Caribe (ALC)

Lineamientos estratégicos:

- Implementar marcos normativos / regulatorios basados en estándares internacionales que ayuden a fortalecer la seguridad cibernética de las instituciones
- Fortalecer a los CSIRT como instituciones públicas al servicio de todos los ciudadanos y las organizaciones, ente adecuado para articular acciones con las fuerzas de orden público.
- Desarrollar estrategias preventivas sobre modelos internacionales y desmotivar el pago de rescates.

NACIONES UNIDAS

CEPAL

REPUBLICA DE CHILE
SENADO

Muchas gracias..!!!!

Rodrigo Mariano Díaz

Certified Information System Security Professional

@ diaz.rodrigo.m@gmail.com

Global Gateway