

DOCUMENTOS DE **PROYECTOS**

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

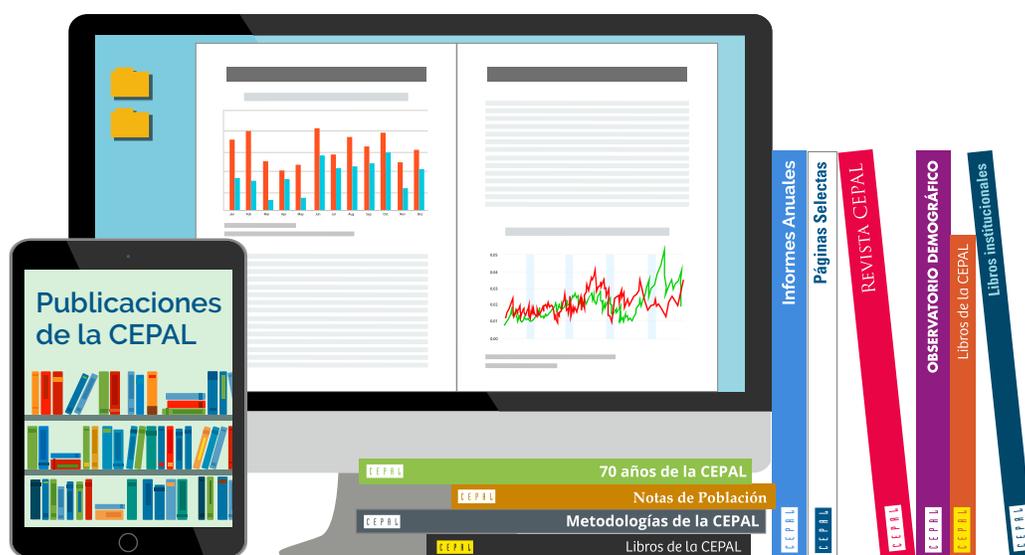
Rodrigo Mariano Díaz



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.

 www.cepal.org/es/publications

 www.cepal.org/apps

Documentos de Proyectos

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

Rodrigo Mariano Díaz



NACIONES UNIDAS

CEPAL

Este documento fue preparado por Rodrigo Mariano Díaz, Consultor de la Unidad de Servicios de Infraestructura de la División de Comercio Internacional e Integración de la Comisión Económica para América Latina y el Caribe (CEPAL), bajo la supervisión de Ricardo J. Sánchez y Jorge A. Lupano, Jefe y Consultor, de dicha Unidad. El estudio fue realizado con el apoyo del programa ordinario de cooperación técnica de la CEPAL, en el marco de las actividades del proyecto de la cuenta de las Naciones Unidas para el Desarrollo 2023 "Transport and trade connectivity in the age of pandemics: contactless, seamless and collaborative UN solutions", en el que participan la Comisión Económica para África (CEPA), la CEPAL, la Comisión Económica para Europa (CEPE), la Comisión Económica y Social para Asia y el Pacífico (CESPAP), la Comisión Económica y Social para Asia Occidental (CESPAO) y la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD).

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 o las de los países que representa.

Publicación de las Naciones Unidas
LC/TS.2022/70
Distribución: L
Copyright © Naciones Unidas, 2022
Todos los derechos reservados
Impreso en Naciones Unidas, Santiago
S.22-00203

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

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

Introducción	7
I. Marco teórico	9
A. Sistemas de ciberinmunidad	10
B. Cultura y ciberseguridad	11
C. Modelos para el abordaje de los ciberataques	12
1. Modelo Cyber Kill Chain.....	12
2. Modelo MITRE ATT&CK	14
3. Modelo Zero Trust.....	17
II. Experiencias globales en <i>Smart Logistics</i>.....	19
A. Ciberseguridad en la logística	19
1. Incidentes de ciberseguridad globales	19
2. Principales debilidades explotadas	22
3. Resiliencia de la red de servicios durante los incidentes ocurridos.....	24
4. Contramedidas	26
B. Aspectos de seguridad de las principales tecnologías implementadas en <i>Smart Logistics</i> : fortalezas y debilidades	30
1. <i>Internet of Things</i>	30
2. Comunicaciones 5G	31
3. Robótica y automatización	32
4. Vehículos autónomos	32
5. <i>Blockchain</i>	34
6. <i>Big Data</i>	35
7. Inteligencia Artificial.....	36
8. Realidad aumentada y realidad virtual.....	38
9. Impresión 3D	38
10. Computación cuántica	40

11. Tecnologías Biónicas	40
III. Gestión global de la ciberseguridad	43
A. Organismos e iniciativas Internacionales	43
1. Programa Mundial sobre Ciberdelincuencia - Oficina de las Naciones Unidas Contra la droga y el delito (UNODC)	44
2. Consejo de Europa – Convenio de Budapest	45
B. Entes Reguladores	45
1. Unión Internacional de Telecomunicaciones (UIT)	45
2. Agencia de la Unión Europea para la Ciberseguridad – ENISA.....	46
C. Organismos de Control	47
1. Interpol.....	47
2. Organizaciones militares	48
3. Organizaciones privadas – Colaboración con organismos oficiales - Gestión pública-privada.....	50
D. Organismos e Iniciativas Regionales.....	50
1. Promovedores de políticas y lineamientos.....	50
2. Entes reguladores.....	51
3. Organizaciones policiales	52
4. Convenios.....	52
IV. El contexto en América Latina y el Caribe.....	53
A. Gobernanza de la ciberseguridad en ámbito público y privado	53
1. Situación en el ámbito privado, empresas internacionales y Pymes.....	54
V. Conclusiones y recomendaciones para la región	57
Bibliografía.....	61
Cuadros	
Cuadro 1	Objetivos de cada etapa del modelo Cyber Kill Chain
Cuadro 2	IA - Distribución de las tareas entre humanos y computadoras
Gráficos	
Gráfico 1	Técnicas utilizadas en los ataques.....
Gráfico 2	Causa raíz de los incidentes totales y cantidad de incidentes por tamaño de organización
Gráfico 3	Porcentaje de Organizaciones de LAC que recibieron ataques según el tamaño de la organización
Gráfico 4	Costo promedio total de una brecha de Seguridad
Gráfico 5	Costo de las brechas de seguridad versus nivel de transformación digital implementada
Gráfico 6	Costo promedio de una brecha de seguridad por nivel de automatización implementado
Gráfico 7	Tiempo promedio para identificar y contener una brecha de seguridad por nivel de automatización
Gráfico 8	Madurez de las tecnologías emergentes.....

Diagramas

Diagrama 1	Etapas del modelo Cyber Kill Chain	12
Diagrama 2	Esquema de interacción de componentes de modelo ATT&CK.....	16
Diagrama 3	Levels of Driving Automation SAE J3016	33
Diagrama 4	Árbol de decisión para el uso de <i>blockchain</i>	35

预览已结束，完整报告链接和二维码如下：

https://www.yunbaogao.cn/report/index/report?reportId=5_31597

