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.

Deseo registrarme

NACIONES UNIDAS

CEPAL

www.cepal.org/es/publications

facebook.com/publicacionesdelacepal

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

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.

Índice

Cuadros

Gráficos

Diagramas

Introducción

La digitalización en su estado actual ha dado lugar al uso de tecnologías exponenciales para facilitar los procesos logísticos a través de la explotación de los datos como uno de los activos mas importantes de las instituciones, generando consecuentemente un aumento en la superficie pasible de riesgo tecnológico.

El objetivo de este estudio, es abordar la problemática de ciberseguridad desde el concepto de la gestión de tales riesgos desde la acción proactiva, a través de modelos disponibles para tal fin, desde la perspectiva individual de las tecnologías disruptivas más utilizadas en logística , y finalmente, desde un enfoque institucional y de gobernanza, considerando que las evidencias indican que todas las instituciones son vulnerables y deberían estar preparadas para afrontar los incidentes de manera similar a los sistemas inmunes biológicos, sugiriendo al mismo tiempo, que prescindir de estas nuevas oportunidades tecnológicas no pareciera ser una opción, sino mas bien un cambio necesario e ineludible para cumplir con las nuevas expectativas del mercado.

I. Marco teórico

La tecnología a lo largo del tiempo ha producido cambios en nuestra sociedad que, a pesar de las controversias, han generado la evolución de la raza humana. La cuarta revolución industrial, según palabras del fundador y director ejecutivo del Foro Económico Mundial, Klaus Schwab, está transformando fundamentalmente la manera en la que vivimos, trabajamos y nos relacionamos unos con otros. Esta transformación será en escala, alcance y complejidad, muy diferente a todo lo experimentado hasta nuestros tiempos. Apoyada en las tecnologías digitales de la tercera revolución industrial y en el crecimiento exponencial del uso de internet, la 4ta revolución industrial está haciendo difusos los límites entre el mundo físico, digital y biológico (Schwab, 2016). Los nuevos caminos que se habilitan llevarán el unwelt[1] de cada humano a niveles que aún no se pueden percibir. Todo aquello que hasta el presente se conocía como autónomo, en la actualidad está conectado, o en breve conectándose, y enviando datos en tiempo real. Es probable que los seres humanos se conecten y envíen datos biológicos en tiempo real en el corto plazo. El cambio que se está experimentando dejó de ser lineal para transformarse en exponencial y el desafío que se avecina es transformase con la tecnología en lugar de transformarse en tecnología (Leonhard, 2016).

Publicaciones recientes de la CEPAL anuncian que las tecnologías claves de la 4ta revolución industrial como Internet de las cosas (*IoT*), la automatización, el *blockchain*, el big data y el cloud computing, están transformando profundamente la logística a nivel global, llevándola a la logística 4.0, demandando la resolución urgente de temas como la alfabetización digital, el costo y la velocidad de acceso a internet, como también de la ciberseguridad (Barleta, Pérez Salas, & Sánchez, 2019). En el desarrollo de dicho estudio se exploró el uso y explotación de los datos como diferenciador, entre las empresas que tomen beneficio de la transformación digital y aquellas que, por no hacerlo, estarán en serio riesgo de subsistir, dejando un interrogante del momento en el que dicha transformación sería

[1] El concepto de Umwelt proviene de una de sus primeras obras, Umwelt und Innenwelt der Tiere (1909). Bajo este término entendía al organismo y su medio ambiente formando un sistema integral. En otras palabras, se trata de la porción del universo que cada ser vivo es capaz de percibir.

clave para la nueva manera de operar dentro de la logística. Estas tres preocupaciones planteadas en una realidad prepandemia se acrecentaron con la aceleración de la digitalización ocurrida como respuesta a las necesidades de continuidad operativa que se produjeron luego de la aparición y el rápido contagio del virus SARS-COV$_2$. El estudio Global Risk Factor del World Economic Forum del año 2021, manifiesta las mismas preocupaciones en cuanto refiere a la tecnología, arrojando concretamente que los riesgos más elevados en probabilidad de ocurrencia son la concentración del poder digital, la inequidad digital y los fallos producidos en materia de ciberseguridad, ocupando estos últimos el cuadrante con mayor probabilidad de ocurrencia e impacto (WEF, The Global Risk Report, 16th Edition, 2021). Es decir, en evaluación de riesgos tecnológicos, los fallos de ciberseguridad son considerados los de mayor factor de riesgo entre los enumerados, estando todos ellos por sobre otro tipo de fallas en las infraestructuras de tecnología.

Tratándose el riesgo en general como una función directa del daño potencial de una amenaza o peligro, y la probabilidad de ocurrencia de estos, entonces se puede concluir que su resultado nunca puede ser nulo, y a sabiendas de que en el mundo hiperconectado las brechas de seguridad pueden ocurrir en fracciones de segundos, a grandes distancias, y sin necesidad de portar herramientas ni armas, sufrir un ataque que vulnere la seguridad cibernética es sólo cuestión de tiempo. Es por ello que el Foro Económico Mundial menciona que las medidas preventivas para cualquier tipo de ciberataque debe incluir la preparación para el momento en que este se produzca, entendiendo que el incidente se producirá en un momento no esperado; hacer una copia de seguridad de los recursos y datos de TI, asegurarse de que haya continuidad en las operaciones en caso de interrupciones de los sistemas informáticos y analizar y capacitar a la organización en el plan de una respuesta cibernética realista es un deber hacer ineludible en los tiempos de la 4ta revolución industrial (WEF, World Economic Forum, 2021). Es clave entonces adoptar la ciberseguridad activamente y, más aún, mejorar la infraestructura de ciberseguridad para tener mayores probabilidades de éxito en las operaciones.

Entre los procesos de adopción o evolución para dar tratamiento a la ciberseguridad, es conveniente contemplar a una parte de los sistemas de ciberdefensa de forma similar a la que los seres vivos se defienden de ataques a su organismo; se podría pensar entonces que los ecosistemas informáticos cuenten con un sistema de ciberinmunidad. Un sistema de estas características atiende la realidad del modelo de organización actual, en constante evolución, pasible de errores e imperfecta.

Al igual que en los organismos vivos, los sistemas ciberinmunes de las organizaciones nunca son perfectos, pudiendo ser vulnerados por virus u otros objetos malignos que pueden atacar funciones de la organización, o incluso atacar el propio sistema inmune. Sin embargo, los sistemas inmunes tienen la fortaleza de adaptarse y aprender, y en este ciclo de aprendizaje continuo, van resultando más efectivos, y van incorporando nuevas y mejores defensas para detener ataques nuevos y desconocidos, llegando a ser capaces de detenerlos, incluso sin conocer con precisión el objetivo ni el mecanismo del ataque. Pensar en ciberinmunidad, permite en caso de ser abatidos por una amenaza, recuperar rápidamente las funciones operativas esenciales de la institución, posibilitando de esta manera, disminuir el triángulo de pérdidas de la curva de resiliencia y, eventualmente, superar los resultados previos al incidente (CEPAL, 2020).

A. Sistemas de ciberinmunidad

Los sistemas de ciberinmunidad son soluciones basadas en inteligencia artificial, más específicamente en técnicas de aprendizaje automático (ML)[2], que no reemplazan las defensas estáticas como antivirus, firewalls, antispam, etc., que se vienen utilizando desde el nacimiento del computador

[2] Machine learning (ML) o aprendizaje automático, es una rama de la inteligencia artificial que permite que las máquinas aprendan sin ser expresamente programadas para ello. Una habilidad indispensable para hacer sistemas capaces de identificar patrones entre los datos para hacer predicciones.

personal, sino un concepto de defensa complementario que se utiliza para minimizar los riesgos cibernéticos (Wlodarczak, 2017), como se expresó anteriormente, en el contexto de evolución tecnológica exponencial como el actual. Al basarse en técnicas de inteligencia artificial, las cuales utilizan metodologías y modelos de estadísticas para predecir el resultado de nuevos valores que requieren del reconocimiento de patrones de comportamiento, las soluciones de ciberinmunidad crecen en efectividad conforme crece la cantidad de patrones de comportamientos que puede analizar el sistema. Por este motivo es un modelo que puede crecer exponencialmente si se cuenta con una mayor recolección de información de tráfico de datos, dando lugar de esta manera a una solución que crece en robustez conforme crece la cantidad de integrantes del sistema. Se puede precisar entonces que, contrariamente al paradigmático concepto de hacer seguridad por oscuridad[3], en estos sistemas que resuelven situaciones más complejas, como predecir o detectar, es clave el esfuerzo común y colaborativo para resolver problemas de ciberseguridad que resulten comunes a una actividad, obteniendo al mismo tiempo beneficios individuales, por ejemplo, detectar situaciones internas sin precedentes gracias al entrenamiento realizado con información global.

B. Cultura y ciberseguridad

Tratándose como se ha mencionado anteriormente en este documento, la cuarta revolución industrial, de una profunda transformación de la raza humana propiciada por las posibilidades que emergen de utilizar tecnologías disruptivas, es importante centrar la atención en las personas en sentido individual y grupal, para entender que el contexto cultural es una gran influencia en la manera de abordar los planes integrales de ciberseguridad, y que en caso de omitir esta particularidad, puede hacer fracasar los esfuerzos tecnológicos que se realicen. Particularmente en América Latina existe una tendencia a minimizar la exposición al riesgo, y más aún al riesgo tecnológico, que podría tener su causa en el desconocimiento de las actividades delictivas que las tecnologías actuales posibilitan. En estudios recientes de CEPAL se ha encontrado que dos tercios de los incidentes de ciberseguridad registrados tienen su origen en errores o distracciones cometidas por los integrantes de la organización a través de la utilización de contraseñas débiles y/o repetidas para las cuentas utilizadas en diferentes servicios (CEPAL, 2021), accediendo a vínculos falsos presentados en distinto tipos de phising, o siendo víctimas de ingeniería social revelando datos sensibles.

Al mismo tiempo, existe una incongruencia en la percepción del impacto que cada miembro de la cadena logística tiene frente a la resiliencia que esta presenta de extremo a extremo. Según una encuesta global del año 2019 realizada por Marsh en conjunto con Microsoft, en las instituciones de LAC que integran cadenas de suministros, el 35% percibe que el riesgo que representan socios o terceras partes es alto o muy alto, pero solo el 18% se ven a sí mismos con ese nivel de riesgo afectando a los demás integrantes (Marsh, 2019). Independientemente del tamaño de la organización y que pertenezcan al sector privado o público, tanto organizaciones pequeñas como medianas o grandes, están con igual probabilidad de ser vulneradas y afectar seriamente la cadena completa. Si bien el atractivo por vulnerar instituciones de mayor poder económico (y de esta manera obtener mayor rédito económico) es una realidad para los cibercriminales, el método masivo que actualmente estos grupos utilizan para conseguir el primer acceso a las redes de sus víctimas, no distingue tamaño y utiliza debilidades técnicas o humanas que la organización aún no ha cubierto, como por ejemplo el envío de mails mencionando servicios masivos como PayPal o Amazon, incitando a los usuarios a abrir vínculos que les permitan luego dejar su carga de ataque y actuar desde ese equipo. A través de resultados que arroja la misma encuesta, se podría deducir que los directivos de LAC aún no dan tratamiento de forma preventiva ni proactiva a la ciberseguridad por

[3] En criptografía y seguridad informática, la seguridad por oscuridad o por ocultación es un controvertido principio de ingeniería de la seguridad, que intenta utilizar el secreto para garantizar la seguridad.

no contar con la percepción real del riesgo que los incidentes de esta índole representan, ya que el 62% de los encuestados respondió que un ataque o incidente cibernético en su empresa sería el principal facilitador para incrementar la inversión en riesgos de esta naturaleza.

C. Modelos para el abordaje de los ciberataques

1. Modelo Cyber Kill Chain

Es conveniente antes de continuar la lectura, presentar brevemente el modelo denominado Cyber Kill Chain desarrollado por Lockheed Martin dentro del entorno Intelligence Drive Defense mediante el cual se podría analizar la actividad técnica que ocurre en la red de datos, y detectar patrones que correspondan a las etapas iniciales de un ataque, evitando de esta manera que el atacante pueda lograr su objetivo (Lockheed Martin, 2021). El modelo Cyber Kill Chain es una de las aproximaciones utilizadas en ciberseguridad para entender y frenar las técnicas de ataque de manera integral, entendiendo que se trata de un proceso y que, como tal, está identificado con diferentes etapas, contando cada una de ellas con objetivos y actividades concretas del lado del atacante. Esta aproximación tiene origen en una técnica militar de la Fuerza Aérea de los Estados Unidos de América conocida por el acrónico F2T2EA que reconocía 6 etapas en un ataque tradicional; **encontrar a continuación (*find*), asegurar (*fix*), rastrear (*track*), elegir el blanco (*target*), abordar (*engage*), evaluar (*assess*)**. Cyber Kill Chain (CKC7), es un modelo adaptado de estas etapas, a las que ocurren durante un ciberataque, especialmente en los casos que estos se tratan de una Amenaza Persistente Avanzada[4] (APT por sus siglas en inglés).

Diagrama 1
Etapas del modelo Cyber Kill Chain

Fuente: Elaboración propia basada en el modelo de Lockheed Martin.

El abordaje se realiza desde la óptica del atacante y del objetivo, correspondiendo a cada una de las fases, como se explicó anteriormente, actividades específicas que pueden ocurrir para que cada figura logre su cometido, es decir las actividades propias del atacante, para lograr el impacto, y las actividades preventivas y reactivas que podría desplegar la víctima para evitar que el atacante logre su objetivo.

Se puede observar que la actividad relacionada con un ciberataque podría ocurrir en segundos y fortuitamente, o de manera dirigida y en semanas, meses o incluso años, pero de todas maneras podrá analizarse desde la óptica del modelo de CKC7 para entender que, en general, no existe manera de evitar un ciberataque, ni tampoco una tecnología o medida específica que pueda evitar los daños, sin embargo aplicando modelos como el de CKC7, se puede abordar de manera global la problemática y pensar que el mejor plan es la suma de acciones simples aplicadas a cada etapa, de manera que se detecte un incidente de manera anticipada, reduciendo, o incluso excluyendo el daño potencial del mismo.

[4] La definición ampliamente aceptada de amenaza persistente avanzada es que se trata de un ataque selectivo de ciberespionaje o cibersabotaje llevado a cabo bajo el auspicio o la dirección de un país, por razones que van más allá de las meramente financieras/delictivas o de protesta política. No todos los ataques de este tipo son muy avanzados y sofisticados, del mismo modo que no todos los ataques selectivos complejos y bien estructurados son una amenaza persistente avanzada. Fuente: Centro Criptológico Nacional de España – Véase en línea en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=47.html.

Cuadro 1
Objetivos de cada etapa del modelo Cyber Kill Chain

Atacante			Víctima	
Etapa	Objetivo	Acciones	Objetivo	Acciones
Reconocimiento: Reconocer al objetivo	Investigar los puntos débiles por los cuales vulnerar a la organización.	Recolección de *mails*. Funcionarios en redes sociales. Información de prensa, lista de participación en eventos.	Reconocer la intención del adversario en caso de que se concrete un ataque.	– Recolectar logs de visitas a páginas webs institucionales. – Utilizar técnicas avanzadas para detectar actividades de reconocimiento.
Militarización: Preparación de la operación	Preparar las herramientas que se utilizaran durante la fase de ataque.	Preparación del *malware*, backdoor, etc. y empaquetado para ser utilizado. Preparación de los formularios que se utilizarán en caso de *phishing*. Designación de la misión.	Detectar la aparición y monitorear las actividades de herramientas constructoras de virus y *malware.* Es la etapa que genera más resiliencia para las organizaciones.	– Realizar análisis completos de *malware.* – Construir herramientas de detección de constructores de *malware*. – Analizar la línea de tiempo relacionada a los *malwares* utilizados. Nuevas apariciones pueden estar relacionados con actividades dirigidas mientras que los *malwares* conocidos pueden asociarse a campañas masivas.
Distribución: Lanzamiento de la operación	Insertar de manera controlada el arsenal tecnológico en la red de la víctima.	Envío de correos maliciosos. Inserción de medios USB con *malware*. Interacción por redes sociales. Acción directa sobre los servidores de web.	Detener el ataque en su etapa más temprana. Tomar como indicador el porcentaje de ataques detectados en esta etapa.	– Analizar el medio de distribución. – Entender los objetivos de ataque y la información disponible en ellos. – Inferir las intenciones del atacante. – Elevar las medidas de detección en los puntos de distribución. – Analizar el horario del ataque. – Recolectar evidencias de correos electrónicos y eventos de los sistemas de información.
Explotación: Obteniendo acceso a la víctima.	Explotar una vulnerabilidad de la víctima para obtener acceso.	– Encontrar vulnerabilidades de *software*, *hardware* o humanas dentro del entorno destino. – Adquirir o desarrollar herramientas *exploits*[a] de día cero. – Desencadenar *exploits* en los servidores de la víctima. – Desencadenar acciones involuntarias de las personas utilizando archivos o vínculos maliciosos.	Utilizar las medidas tradicionales de defensa para incrementar la resiliencia, y las capacidades estratégicas diseñadas para frenar acciones desconocidas.	– Ejecutar un plan de concientización en ciberseguridad a todos los funcionarios de la organización. – Realizar periódicamente pruebas controladas de *phishing*. – Capacitar al equipo de desarrollos en técnicas de codificación seguras. – Buscar regularmente vulnerabilidades en la instalación y probar controladamente las medidas implementadas (*Pen Test*). – Implementar en los puestos de trabajo de usuarios restricciones de privilegios elevados, bloquear la ejecución de código desconocido y habilitar auditoría de eventos para tareas forenses.

Atacante			Víctima	
Etapa	Objetivo	Acciones	Objetivo	Acciones
Instalación: Estableciendo acceso permanente a la instalación de la víctima.	Desplegar en la instalación vulnerada un conjunto de herramientas que le permitan al atacante acceso continuo.	– Instalar webshell en los servidores web. – Implementar un o un conjunto de *backdoors*[b]. – Crear puntos de persistencia mediante servicios.	Detectar y detener actividades anómalas en los extremos de la instalación.	– Alertar y bloquear actividades no estandarizadas en los directorios de instalación habituales. – Analizar los privilegios que requieren los *malwares* detectados. – Alertar y analizar la creación de archivos. – Determinar la antigüedad de los *malwares* identificados. – Verificar los certificados de los archivos que contengan firma.
Comando y control (C2): Accediendo en forma remota los controles implantados.	Manipular de manera remota la instalación de la víctima utilizando canales habilitados por el *malware* instalado.	– Habilitar canales de comunicación bidireccionales entre la instalación de la víctima y la infraestructura de C2 del atacante. – + Los canales habitualmente utilizados son los protocolos de web, DNS[c], y correo electrónico. – + La infraestructura C2 puede ser propia o la instalación de otra víctima.	Frenar operaciones maliciosas y filtración de información en la última línea de defensa.	– Analizar el *malware* detectado con el fin de encontrar infraestructuras de C2. – Reforzar la seguridad de la red de comunicaciones consolidando las salidas a internet en la menor cantidad de puntos posibles y utilizando *proxies*[d] para todo tipo de tráfico de salida. – Personalizar los bloqueos de acceso a infraestructura de C2 en los *proxies*. – Analizar periódicamente las nuevas infraestructuras de C2.
Acciones sobre los objetivos: Logrando el objetivo de la misión**.**	Cumplir la meta de la misión a través del acceso deliberado a los equipos de la víctima.	– Recolectar credenciales de usuarios. – Escalar privilegios. – Reconocimiento interno de la instalación. – Movimiento lateral en el entorno de la víctima. – Recolectar y exportar datos. – Destruir sistemas completos. – Sobrescribir o corromper datos. – Modificar datos subrepticiamente.	Detectar que se está frente a un ataque que ha llegado a esta etapa tan pronto como sea posible. Cuanto más tiempo se demore en reaccionar, mayor será el daño sufrido.	– Establecer un manual estratégico de respuesta a incidentes. Incluir el compromiso ejecutivo y plan de comunicaciones. – Detectar exfiltración de datos, movimiento lateral y uso de credenciales no autorizado. – Responder inmediatamente a todas las alertas. – Disponer previamente de agentes desplegados para un rápido análisis forense. – Capturar de paquetes de red para recrear la actividad. – Realizar una evaluación de daños con especialistas técnicos.

Fuente: Elaboración Propia basada en el Modelo Cyber Kill Chain - Proactively detect persistent threats: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

[a] Un exploit es un programa informático, una parte de un *software* o una secuencia de comandos que se aprovecha de un error o vulnerabilidad para provocar un comportamiento no intencionado o imprevisto en un software, *hardware* o en cualquier dispositivo electrónico. Fuente: Panda Security. Exploit: ¿sabes qué es y cómo funciona? - https://www.pandasecurity.com › security-info › exploit.

[b] Se denomina *backdoor* a una secuencia de programación que habilita acceso a un sistema sin ser advertido por el usuario y evita los algoritmos de autenticación de acceso.

[c] El DNS (Domain Name System, Sistema de Nombres de Dominio) es un conjunto de protocolos y servicios que permite a los usuarios utilizar nombres en vez de tener que recordar direcciones IP numéricas. Fuente: https://www.ujaen.es/servicios/sinformatica/catalogo-de-servicios-tic/nombres-de-dominio-dns.

[d] Un proxy es un ordenador intermedio que se usa en la comunicación de otros dos. La información (generalmente en Internet) va directamente entre un ordenador y otro. Mediante un proxy, la información va, primero, al ordenador intermedio (proxy), y éste se lo envía al ordenador de destino, de manera que no existe conexión directa entre el primero y el último. Fuente: ¿Qué es un proxy y para qué sirve? https://mi.certerus.com/knowledgebase/124/iQue--es-un-Proxy-y-para-que-sirve-.html.

2. Modelo MITRE ATT&CK

La asociación MITRE sin fines de lucro, de Estados Unidos de América con sus orígenes en 1958 en el Massachusets Institute of Technology ha desarrollado en el año 2013 un método en forma de matriz para modelar un ciberataque, el cual lleva por nombren ATT&CK (Advanced Tactics and Technics & Common Knowledge). La base de ATT & CK es el conjunto de técnicas y sub-técnicas que representan acciones que los ciberatacantes pueden ejecutar para lograr objetivos. Esos objetivos están representados por las categorías de tácticas a las que pertenecen las técnicas y sub-técnicas. Esta representación relativamente simple logra un equilibrio útil entre detalle técnico y el contexto en torno al que ocurren las acciones a nivel táctico (MITRE Corporation, 2020). A diferencia del modelo Cyber Kill Chain, en las tácticas agrupadas en categorías que pueden ser asociados a los pasos de un ataque, pueden no estar presentes todos los pasos y su cronología puede ser distinta al orden en el que se presentan en la matriz. Desde un punto de vista de alto nivel, ATT & CK está compuesto por la siguiente estructura:

- **Tácticas**: que denotan metas tácticas de los atacantes a corto plazo;
- **Técnicas**: que describen los medios por los cuales se logran los objetivos tácticos;
- **Sub-técnicas**: que describen medios más específicos por los cuales se logran las metas tácticas a bajo nivel; y
- Documentación de técnicas utilizadas durante los ataques, sus procedimientos y otros metadatos.

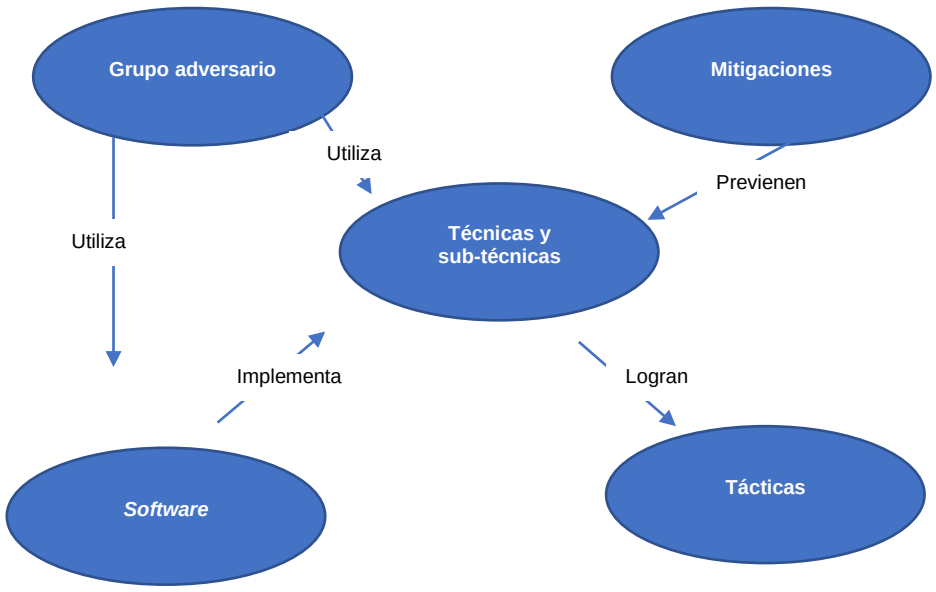
Dentro de ATT & CK, como se enumeró, se puede encontrar una vasta cantidad de documentación sobre diferentes aspectos que pueden facilitar el análisis y tratamiento, tanto de una problemática en curso como de manera preventiva. Dentro de ella se encuentran:

- **Procedimientos**, refiriéndose con este término a las implementaciones específicas que los adversarios han utilizado para ejecutar técnicas o sub-técnicas;
- **Grupos**, que se definen como conjuntos de intrusiones, grupos de amenazas, grupos de actores o campañas con nombre que normalmente representan actividad de amenaza persistente. ATT & CK se centra en grupos APT, aunque también puede incluir otros grupos avanzados, como los actores motivados financieramente;
- ***Software***, que representa una instanciación de una técnica o sub-técnicas; los grupos adversarios durante las intrusiones pueden usar técnicas directamente o diferentes tipos de *software* que implemente técnicas; el *software* se divide en dos categorías, que podrían desglosarse aún más, pero la idea detrás de la actual es mostrar cómo los adversarios usan herramientas y *software* legítimo para realizar acciones, al igual que lo hacen con el *malware* tradicional:
  - Herramientas, *software* comercial, de código abierto o disponible públicamente, que podría ser utilizado por un equipo de prueba o un adversario, incluyendo tanto *software* que se obtiene con un fin especifico (por ejemplo, PsExec, Metasploit, Mimikatz), como el *software* que está disponible como parte de un sistema operativo ya presente en el entorno técnico bajo análisis (por ejemplo, utilidades de Windows como Net, Netstat, lista de tareas, etc.);
  - *Malware*, *software* comercial de código cerrado personalizado o de código abierto, destinado a ser utilizado con fines maliciosos por personas o grupos adversarios (por ejemplo, PlugX, CHOPSTICK, etc.);
- Mitigaciones, estas en ATT & CK, representan conceptos de seguridad y clases de tecnologías que se pueden utilizar para evitar que una técnica o sub-técnicas se ejecute con éxito. Existen 41 mitigaciones en ATT & CK for Enterprise que incluyen casos como

aislamiento de red y zona de pruebas de aplicaciones, copia de seguridad de datos, prevención de ejecución, entre otras; las mitigaciones son independientes de productos comerciales y solo describen categorías o clases de tecnologías que podrían utilizarse, sin referirse a soluciones específicas (MITRE Corporation, 2020).

A modo de resumen, el diagrama 2 muestra un esquema de interpretación de los componentes del modelo MITRE ATT &CK.

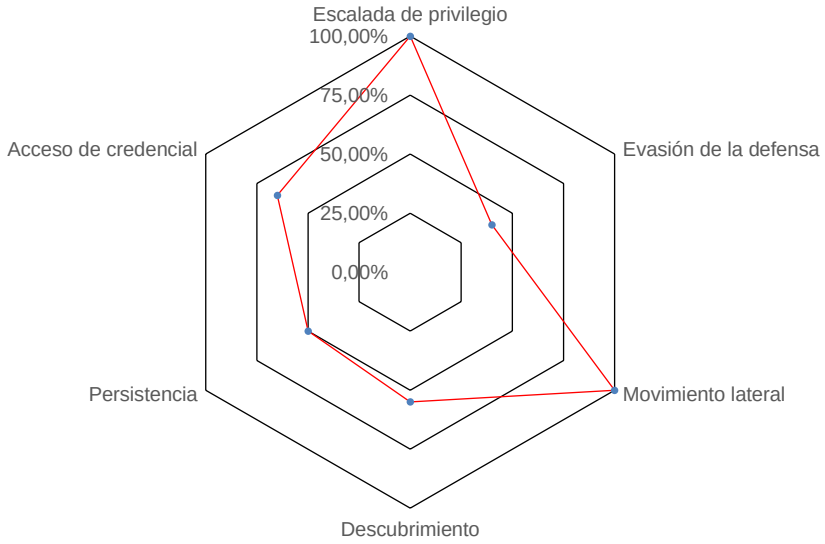
Diagrama 2
Esquema de interacción de componentes de modelo ATT&CK



Fuente: Elaboración propia basada en documentación de organización MITRE.

A continuación, puede observarse en qué porcentaje de los incidentes reportados durante los últimos 12 meses previos a julio de 2021, se han utilizado las diferentes técnicas del modelo MITRE (Coveware, 2021). Puede observarse una baja utilización de la técnica de evasión de la defensa, lo cual podría reflejar la baja capacidad que actualmente tienen las organizaciones para detectar un ataque; es por este motivo entre otros factores que, durante el año 2020, según un informe que la firma IBM presenta anualmente sobre los costos de las brechas de seguridad, llevó en promedio 212 días a las organizaciones descubrir las irrupciones de seguridad informática (IBM Inc., 2021).

Gráfico 1
Técnicas utilizadas en los ataques
(En porcentajes)



Fuente: Elaboración propia basada en datos obtenidos de Coveware.

En ambos modelos de ataques presentados previamente, puede apreciarse que los atacantes podrían tener acceso recurrente a la infraestructura vulnerada y pasar inadvertidos si no existen las medidas de detección que alerten esta situación. De hecho, la principal preocupación del intruso es pasar inadvertido y borrar sus huellas antes de retirarse, excepto que su objetivo sea bloquear las operaciones.

3. Modelo Zero Trust

El modelo de seguridad Zero Trust fue desarrollado en 2010 por Forrester y se trata de un conjunto de pautas de diseño de sistemas y una estrategia coordinada, basada en el paradigma de que las amenazas existen tanto dentro como fuera de los límites tradicionales de la red. Zero Trust cuestiona repetidamente la premisa de que los usuarios, dispositivos y demás componentes integrantes de un sistema informático, deben confiar según la ubicación en la red. Para llevar este concepto adelante, se incorpora un monitoreo integral de seguridad; controles de acceso granulares, dinámicos y basados en el riesgo; y la gestión de la seguridad del sistema de manera coordinada y automática para lograr la protección de los activos críticos (datos) en tiempo real dentro de un entorno de amenazas dinámico. Este modelo de seguridad centrado en los datos permite aplicar el concepto de acceso con mínimo privilegio para cada decisión de acceso, donde se cuestiona permanentemente quién, qué, cuándo, dónde y cómo se está solicitando acceso al objeto para permitir o denegar la acción (CISA, 2021).

II. Experiencias globales en *Smart Logistics*

La literatura actual respecto a la eficiencia de las cadenas logísticas globales considera los impactos de todas las acciones desde el momento que la carga se crea en origen hasta llegar a manos del cliente. En un estudio reciente, Álvarez y Sánchez exhiben las oportunidades y desafíos que la región presenta para el advenimiento de la logística inteligente, y mencionan las tecnologías influyentes en el sector para los próximos años. En el presente apartado, se analizarán los desafíos y ventajas de estas tecnologías desde el punto de vista de la ciberseguridad, comenzando por experiencias y eventos ocurridos a nivel global, y como las organizaciones se repusieron, o incluso se potenciaron luego de dichos eventos.

A. Ciberseguridad en la logística

1. Incidentes de ciberseguridad globales

En el Boletín FAL número 382 publicado en el mes de noviembre de 2020 por CEPAL (CEPAL, 2020), se consideran aspectos técnicos de la seguridad aplicable al alcance interno de las organizaciones y se describen acciones internas para reducir el riesgo cibernético. En esa instancia se citan algunos incidentes y las pérdidas económicas junto con otros impactos asociadas a ellos. Los más significativos son el recordado evento de 2011 del Puerto de Amberes en Bélgica, víctima de un ataque encargado por un cártel de droga dirigido contra sistemas terminales que posteriormente fueron comprometidos por piratas informáticos, y utilizados para liberar contenedores sin que las autoridades portuarias lo notaran; se incautaron en este incidente, drogas ilícitas y contrabando por un valor aproximado de 365 millones de dólares además de armas de fuego. También se puede citar el ataque de *ransomware* recibido por MAERSK en junio de 2017 que provocó una disrupción operativa con pérdidas por u$s 264.000.000. Como se explicará más adelante, luego de este incidente, Maersk llevó adelante una de las iniciativas más importantes de *Smart Logistics* implementando junto a IBM la solución de Tradelens, que se ocupa de la gestión global de documentación de la carga, de extremo a extremo, en una solución distribuida que utiliza *blockchain* para la trazabilidad de dichos documentos. En el año 2020 MSC sufrió un incidente provocado por una pieza de *software* maliciosa, provocando disrupción en los sistemas de

desintermediación denominados MyMSC. El ataque no provocó detenciones operativas en la compañía, pero dejó sin el acceso des intermediado a los servicios de clientes finales.

El año 2021 no fue la excepción en incidentes para la logística con eventos que siguen al ocurrido en octubre de 2020 en los servicios en línea de la Organización Marítima Internacional. Los ataques de *ransomware* sufridos por las navieras Bourbon y GazOcean en el mes de abril (Mundo Marítimo, 2021), fueron la antesala de los más difundidos ocurridos en 2021 en el puerto de Houston y en la firma Transnet SOC Ltd. en Sudáfrica. El caso del puerto de Houston tiene un giro importante debido a que la Autoridad Portuaria puso en marcha el Plan de Seguridad, armado según las leyes de Seguridad del Transporte Marítimo (MTSA), logrando que ningún dato o sistema operativo se vea afectado. El ataque se inició en una vulnerabilidad descubierta recientemente en un producto que la organización utiliza para la gestión de contraseñas de los usuarios (Katabella, 2021). No resultó de la misma manera el caso de Transnet SOC Ltd. donde las operaciones del puerto debieron cambiarse a modo manual luego que se declarara *"fuerza mayor"* el día 22 de julio de 2021. El ataque se atribuye a grupos operadores de *ransomware* utilizando cadenas conocidas bajo los nombres *"Death Kitty"*, *"Hello Kitty"* o *"Five Hands"*, y que ya se habían observado en ataques realizados aprovechando las vulnerabilidades del producto de monitoreo de la firma Sonicwall publicado algunos meses antes. No se han difundido aún evaluaciones económicas del evento, pero como es conocido, solamente la terminal de Durban operada por la compañía se ocupa del movimiento de más del 60% de los contenedores de todo el país y opera como nodo de intercambio con rutas de Oriente Medio, el Océano Indico y Australia (Gallagher & Burkhardt, 2021). Además de la terminal de Durban que detuvo por completo sus operaciones por la salida de servicio a causa del ataque de su sistema NAVIS SPARC N4, fue afectada parcialmente por el incidente, la terminal de Ciudad del Cabo que pudo continuar sus operaciones con registración manual (García, 2021).

Dentro de la cadena de provisión de alimentos, en junio la firma JBS USA había pagado un rescate de 11 millones de dólares para recuperarse de un ciberataque que llevó al cierre de todas sus unidades operativas de procesamiento de carne. Si bien se había ya recuperado la operatividad en sus servicios de IT, el CEO de la compañía decidió abonar el rescate para recuperar los datos secuestrados y evitar su difusión, con el consecuente daño que la firma consideró que podría causar a sus clientes (Fung, 2021).

La logística ocupa en general el segundo o tercer lugar de los rubros más atacados según los informes que anualmente publica la firma IBM, por su atractivo económico, pero también por el efecto dominó a otras actividades. Pero el rubro que en supremacía afecta a los demás sectores con cada afectación, y por supuesto a la logística, es el correspondiente a las infraestructuras críticas. Dentro de esta actividad se pueden mencionar los más notorios de los últimos años, como, por ejemplo, el recibido en 2019 por la compañía mexicana Pemex que afectó al 5% de los equipos de la compañía y, si bien la empresa petrolera no debió interrumpir sus operaciones, ya advertía y daba lecciones aprendidas para este tipo de organizaciones (Harán J. M., 2019). Mas tarde, en 2020, la compañía Electrobras Termonuclear S.A. proveedora de servicios de energía eléctrica, se vio afectada por *ransomware* en sus sistemas administrativos. También el mismo año y rubro registro la exfiltración de una gran cantidad de datos (1000 GBytes) de la firma Copel S.A.

Las necesidades de adaptación y los esfuerzos por brindar servicios con mejor experiencia de usuario y cada vez más eficientes, siguen avanzando en un terreno donde pareciera que todavía no se logra evaluar correctamente los riesgos asociados a la tecnología, y tampoco se logra actuar con suficiente velocidad partiendo de las lecciones aprendidas de eventos ya ocurridos. Es así como el 7 de mayo de 2021 el grupo de ciber atacantes conocido DarkSide, logró dar en el blanco de su objetivo, perpetrando un ataque sin precedentes a la compañía Colonial Pipeline CO. Si bien el ataque se originó en las redes administrativas, la dirección determinó detener la totalidad de las unidades operativas que controlan los 8850 kilómetros de oleoducto que unen el estado de Texas con el de Nueva York, para evitar mayores daños, lo cual dejó entrever que la situación de las redes operacionales de la

organización, no era diferente a la realidad de muchas, y es que la creencia de larga data de que las operaciones están totalmente aisladas de los sistemas de datos no es real, y es , en parte debido a la vertiginosa actualización que las redes de OT de manera similar a la de las redes administrativas, con el agravante de que la velocidad con la que ocurren los cambios en las redes de OT en estos días es muy superior a la forma en la que se vienen dando durante las últimas décadas en las redes tradicionales de tecnología de la información. Las largas filas de automovilistas en las estaciones de servicio, fue el primer efecto derivado de la decisión tomada por Colonial Pipeline, que controla casi la mitad del combustible para aviones y el diésel que fluye a lo largo de la costa este de Estados Unidos. Lo hizo por la preocupación de que el *malware* que había infectado sus funciones de back-office podía dificultar la facturación del combustible entregado o incluso propagarse al sistema operativo que controla las operaciones del oleoducto (Sanger & Perlroth, 2021). Las consecuencias de este ataque a una infraestructura crítica tan importante como Colonial Pipeline llevaron a que la Administración Federal de Seguridad de Autotransportistas (FMCSA, por sus siglas en inglés) declarara la emergencia regional en Alabama, Arkansas, Washington D.C., Delaware, Florida, Georgia, Kentucky, Luisiana, Maryland, Misisipi, Nueva Jersey, Nueva York, Carolina del Norte, Pensilvania, Carolina del Sur, Tennessee, Texas, y Virginia (Harán J. M., 2021).

Durante años, funcionarios públicos y privados relacionados con organizaciones que atienden infraestructura crítica, han realizado simulaciones elaboradas de un ciberataque dirigido a la red eléctrica o los gasoductos en los Estados Unidos, imaginando cómo respondería el país. Pero cuando llegó el momento real, sorprendió que:

- el atacante resultó ser una red de extorsión cibernética en lugar de un gobierno hostil o grupo terrorista,
- la finalidad del ataque no era interrumpir la economía deteniendo una infraestructura crítica, sino mantener a modo de rehén los datos corporativos para exigir un rescate económico.

Luego ocurrió un escenario muy diferente al de las simulaciones de escritorio y sus consecuencias en cascada resultaron de las más inesperadas, incluso el punto de partida se puede considerar como un ataque relativamente poco sofisticado. Los Departamentos de Energía y Seguridad Nacional encontraron que el país solo podía permitirse otros tres a cinco días con el oleoducto Colonial cerrado antes de que los autobuses y otros transportes masivos tuvieran que limitar las operaciones debido a la falta de combustible diésel. Las fábricas químicas y las operaciones de refinería también cerrarían porque no habría forma de distribuir lo que producían. Y aunque los asesores del gobierno nacional enumeraron esfuerzos para encontrar formas alternativas de transportar el combustible para aviones y otros transportes por la costa este, ninguno se pudo poner en marcha de inmediato.

Finalmente, luego de pagar a los extorsionadores casi $ 5 millones de dólares en moneda digital para recuperar los datos, el proceso para descifrarlos y volver a encender el oleoducto fue agonizantemente lento, ya que nunca se había detenido por completo un oleoducto de esa magnitud, lo que significó varios días antes de que la costa este volviera a la normalidad. Para la administración pública, el evento resultó ser una semana peligrosa en la gestión de crisis, razón por la que se publicó una orden ejecutiva de larga gestación que, por primera vez, busca exigir cambios en la ciberseguridad, incluyendo la acción directa para contraataque al grupo detrás de la acción, lo cual desencadenó en el apagado de los sitios de Internet de DarkSide y varios otros grupos de *ransomware*, incluido Babuk, que atacó al departamento de policía de Washington D.C., anunciando públicamente su retiro de la acción (Sanger & Perlroth, 2021).

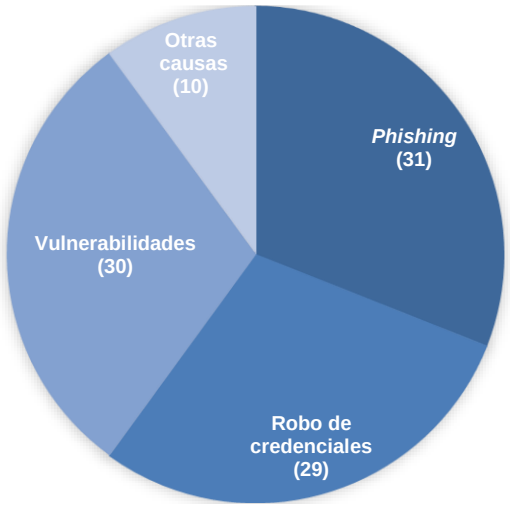
También se debe considerar dentro de la ciberseguridad, fallos de *software* expuestos durante el estado de producción de la infraestructura que atentan a la continuidad y el rendimiento de esta, revelando defectos de diseño cuya resolución de base resulta altamente compleja. Debido al perjuicio

económico que provocan estos casos para las organizaciones, algunas veces se recomienda la consideración de aplicar soluciones que, pudiendo estimarse inicialmente de tipo transitoria, finalizan adoptándose de rutina dentro del plan de actualizaciones ordinarias de la organización. En el año 2015 la empresa aeronáutica Boeing detectó en su modelo 787 Dreamliner un error en la programación de las unidades de control de los cuatro generadores eléctricos principales que portan dichas aeronaves, que hace que si estas permanecen encendidas durante 248 días entren en un modo de protección contra fallos que pararía los cuatro generadores, pudiendo producirse la pérdida de control del avión debido a que este fallo se puede producir en cualquier fase del vuelo. Esto ocurre cuatro años después de que el Boeing 787 comenzase a operar de manera comercial, extendiéndose su uso en un importante número de empresas aerocomerciales. Boeing publica esto al mismo tiempo que comunica que el estudio de la resolución del caso se encuentra en laboratorio, por lo que se impondría la inoperatividad de esos aviones, con los consecuentes perjuicios económicos que esto significa para la actividad. Asimismo, la empresa fabricante informa que esta falla se detecta luego que las unidades de control permanecen encendidas durante 248 días; ante esta comunicación la Autoridad Federal de Aviación de los Estados Unidos publica una orden de efecto inmediato que obliga a apagar y encender todos los Boeing 787 matriculados en los Estados Unidos al menos una vez cada 120 días, medida que es adoptada por sus pares del resto del mundo. Con independencia que sería extremadamente raro que las cuatro unidades de control fueran encendidas a la vez y que permanezcan encendidas durante esos 248 días, y de hecho el fallo solo se ha detectado en pruebas de laboratorio, esta medida, se convierte en un caso seguridad preventiva.

2. Principales debilidades explotadas

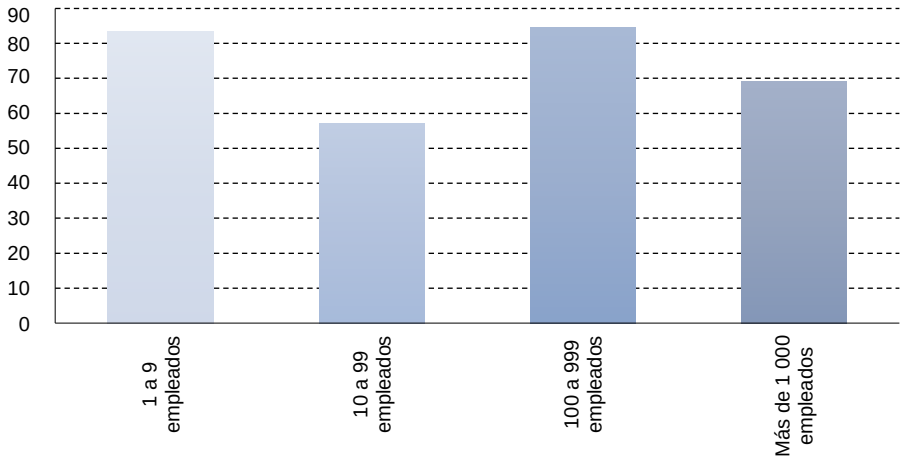
En estudios recientes de CEPAL se ha encontrado que el 72% de las organizaciones de logística de la región han recibido un ciberataque en los últimos 12 meses (CEPAL, 2021) revelando al mismo tiempo una distribución relativamente homogénea en relación al tamaño de las organizaciones, exponiendo además que las principales debilidades que los atacantes logran explotar, corresponden a diferentes técnicas de phishing en el 31% de los casos, robo de credenciales en el 29% de las oportunidades (sea por exfiltración de datos de sitios vulnerados en los cuales los usuarios utilizaban la misma contraseña que el sitio atacado o por deducción de la misma por su simpleza), un 30 % para el aprovechamiento de vulnerabilidades técnicas de los productos de *hardware* y *software* , totalizando un 10% otras causas. Es decir que como se comentara en la sección 1.2, en el 60% de los casos, la causa raíz de la irrupción indeseada dentro de las redes, son las personas dentro de la organización.

Gráfico 2
Causa raíz de los incidentes totales y cantidad de incidentes por tamaño de organización
(En porcentajes)



Fuente: Elaboración propia basada en datos de Symantec y encuesta realizada por CEPAL.

Gráfico 3
Porcentaje de Organizaciones de LAC que recibieron ataques según el tamaño de la organización
(En números y porcentajes)



Fuente: Elaboración propia basada en datos de Symantec y encuesta realizada por CEPAL.

Estas cifras toman en cuenta aquellas instituciones que descubren que fueron atacadas y lo denuncian, pero en muchas oportunidades las organizaciones no llegan a hacer pública la información de haber sido víctimas de un ataque, o peor aún, algunas veces, ni lo llegan a notar. Esto ocurre principalmente cuando el objetivo del atacante es el robo o la manipulación de la información sin afectar las operaciones de la víctima. El caso citado del puerto de Amberes podría asociarse a este tipo de actividad.

Al analizar las vulnerabilidades utilizadas como vector de ataque durante el primer semestre de 2020, se ha encontrado que solo el 5% corresponden a debilidades descubiertas en los años 2019 y 2020, y solo un 15% en 2018 (Checkpoint LTD., 2020). Es decir que el 80% de las fragilidades explotadas, se habían anunciado al menos 2 años antes y sus remediaciones estaban disponibles

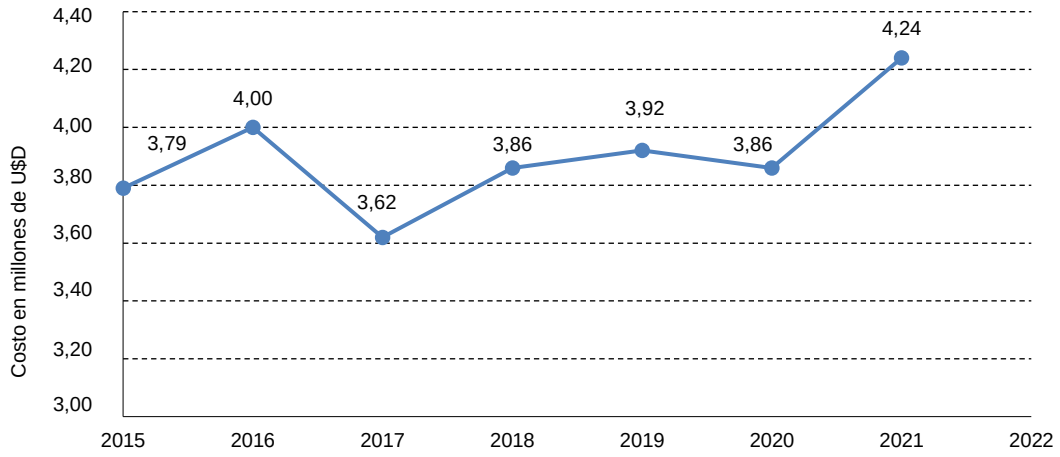
desde entonces, lo cual denota las dificultades que las organizaciones enfrentan en mantener actualizados el *software* y el *hardware* en sus instalaciones.

3. Resiliencia de la red de servicios durante los incidentes ocurridos

A diferencia de lo que ocurrió en las últimas dos décadas del siglo XX, los atacantes detrás de los eventos que atentaron contra la ciberseguridad de las organizaciones desde el año 2000 en adelante, han perseguido mayoritariamente fines lucrativos. Al principio fueron fraudes en línea, con monetizaciones inmediatas relativamente pequeñas, para luego evolucionar a las campañas masivas de *ransomware*, lo cual ha derivado en situaciones cada vez más complejas de resolver, obligando a las víctimas a ofrecer sumas elevadas de dinero para subsanar dichas situaciones, en algunos casos retomar la operatividad, y en otros evitar la divulgación de información sensible, cuando no una combinación de ambas.

Las amenazas han dejado de ser individuos en algún garaje tratando de demostrar sus habilidades y satisfaciendo su ego, para transformase en organizaciones productivas con métodos y procedimientos que, como en toda industria lucrativa, evoluciona para ser cada vez más eficiente y efectiva en la monetización directa o el logro de objetivos contratados por terceros. Los rescates solicitados en el segundo trimestre del año 2021 han promediado la suma de u$s 136.576, habiendo pasado por un pico de u$s 230.000 en el tercer trimestre del año anterior. Lejos quedan estos valores de los costos reales que dejan los incidentes, ya que se ha determinado que el promedio de tiempo con operaciones detenidas luego de un ataque de *ransomware* es de 23 días para 2021, cifras menores a 2020, donde la misma medición ascendía a 41 días. Según el informe anual mencionado previamente que IBM realiza sobre los costos de las brechas de seguridad ocurridos durante el año 2020, el costo total de las brechas de seguridad ascendió en promedio a 4.24 millones de dólares, es decir un 9.8% más que el costo promedio de 3.86 millones de dólares calculado para 2019 (IBM Inc., 2021). En el sector de logística, este promedio ha sido de 3.75 millones de dólares para 2021.

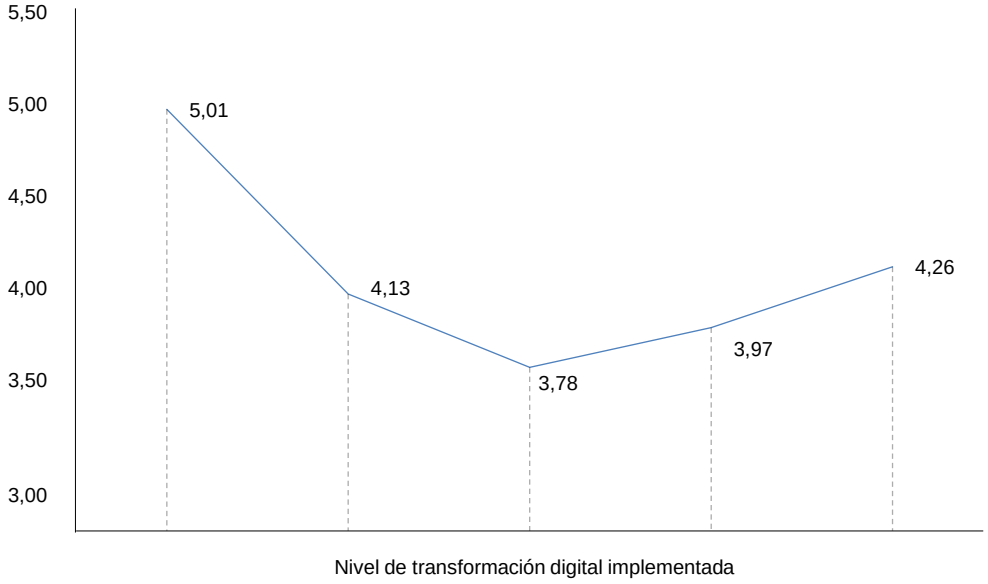
Gráfico 4
Costo promedio total de una brecha de seguridad
(Costo en millones de USD)



Fuente: Elaboración propia basada en datos de IBM Inc.

Un dato pertinente al objetivo principal del presente documento es que los costos de las brechas de seguridad han sido más elevados en las organizaciones que aún no han comenzado un proceso de transformación digital frente a aquellas que se han transformado por completo.

Gráfico 5
Costo de las brechas de seguridad versus nivel de transformación digital implementada
(Costo en millones de USD)



Fuente: Elaboración propia basada en datos de IBM Inc.

Se puede interpretar entonces, que las organizaciones que han emprendido el camino de la transformación digital y en este proceso hayan considerado de manera integral y actualizada a la ciberseguridad, han sido impactadas con costos significativamente menores en los casos de haber sido afectadas por eventos de esta naturaleza.

El impacto económico que enfrentan las organizaciones en un evento de seguridad es solo una de las variables a evaluar, pero puede no ser la más representativa; un ejemplo de estos casos podría considerarse el ataque a Colonial Pipeline descripto anteriormente, o casos de infraestructura crítica u organizaciones de la salud. En este último rubro, ha sido noticia en el mes de septiembre de 2021, que el Springhill Medical Center de Estados Unidos enfrenta una demanda presentada por una paciente que dio a luz en julio de 2019, ya que las circunstancias en las que ocurrió el parto podrían haber sido afectadas porque el centro médico se encontraba bajo los efectos de un ataque de *ransomware*, lo cual podría haber sido determinante en el fallecimiento de la bebé, ocurrido 9 meses más tarde (Poulsen, McMillan, & Evans, 2021).

Según Kiersten E. Todt, directora gerente de la organización sin fines de lucro Cyber Readiness Institute, refiriéndose al incidente del oleoducto, las instituciones están pensando demasiado en las amenazas, cuando todavía no están haciendo lo básico para proteger la infraestructura crítica (Sanger & Perlroth, 2021), ya que los expertos en ciberseguridad que analizaron de cerca el caso, señalan que Colonial Pipeline nunca habría tenido que cerrar su oleoducto si hubiera tenido más confianza en la separación entre su red comercial y las redes de control operativo. Además, preocupa que quedó expuesto el bajo estado de resiliencia, no solo a las superpotencias, sino también a los terroristas y los ciberdelincuentes, que aprendieron lo poco que se necesita para incitar al caos en una gran parte de un país, incluso si no irrumpen directamente en las redes de control de las distribuciones de electricidad, combustible, agua o gas.

El episodio de Colonial Pipeline CO denota que una amenaza proveniente de grupos de ciberdelincuentes privados y que a menudo afectan a organizaciones con fines lucrativos puede despertar tensiones políticas internacionales en torno al tratamiento que cada estado le dé, no solo a

no combatir la ciberdelincuencia, sino a albergarla, o incluso propiciarla, y la falta de esfuerzos internacionales por desarticular redes de estas características. En otras palabras, las acciones no autorizadas ejecutadas virtualmente ocurren desde una ubicación física con su correspondiente jurisdicción hacia otra, afectándola mínimamente de manera económica, donde la falta de acción en la jurisdicción de origen puede provocar daños internacionales que pueden derivar en acciones que vayan mucho más allá del ámbito virtual.

El tiempo que ha llevado descubrir una brecha de seguridad ha resultado en un promedio de 212 días para 2021. Si a este tiempo se le adiciona el promedio de 75 días en contenerla, da un total de 287 días, cifra que corresponde a 7 días más que en 2020. Es decir que una brecha de seguridad promedio ocurrida el 1ro de enero de 2021, no pudo ser contenida hasta el día 14 de octubre. Como se verá con mayor nivel de detalle más adelante, tanto en contramedidas como en la sección destinada a inteligencia artificial, dentro de las tecnologías disruptivas, las estadísticas indican que nivel de automatización de las herramientas utilizadas y el enfoque de implementación de sistemas del tipo de ciber inmunidad, se encuentran presentes en las organizaciones que han demorado menos en descubrir y contener una brecha, promediando un total de 247 días para el ciclo completo, 184 días para descubrir y 63 días para contener la misma. En el extremo opuesto, quienes no tienen ningún sistema automatizado para detección de brechas de seguridad han visto este ciclo extendido a un total de 324 días (IBM Inc., 2021).

Como conclusión respecto a la resiliencia frente a los incidentes ocurridos en logística, de los cuales se han expuesto algunos de los que se han dado a conocer públicamente, se puede afirmar que, tanto a nivel organización como para el resto de los integrantes de la cadena logística, contar con un Sistema de Gestión de Seguridad de la Información (SGSI), es la medida rectora general que, impulsada desde la autoridad máxima de la organización, ha permitido minimizar el impacto operativo. Específicamente el Plan de Continuidad de Negocio o Bussiness Continuity Plan (BCP), que es parte del SGSI, ha sido el diferenciador para alinear las acciones en un evento como el ocurrido a MAERSK en el año 2017 o a Transnet LTD en 2021 y de esta manera minimizar el impacto operativo. Si bien el objetivo del documento no es extenderse sobre los detalles del BCP, es pertinente destacar que la correcta especificación de parámetros que determinan la declaración de la emergencia o, dicho de otra forma, que se debe poner en marcha el BCP, es fundamental para evitar demoras o dudas en momentos de crisis, como también lo es la gestión oportuna de las comunicaciones privadas y públicas relacionadas con el caso. Esta práctica debería reforzarse en la región ya que en el informe de CEPAL sobre el estado de la ciberseguridad en LAC (CEPAL, 2021) se ha encontrado que solo el 22% de las organizaciones realizan periódicamente una prueba de esta naturaleza.

4. Contramedidas

Como lo expresa generalmente la literatura académica, se enuncia en este documento y las realidades operativas lo confirman, preparar a cada organización para enfrentar los retos que plantea la ciberseguridad en la actualidad, es una tarea que debe planificarse cuidadosamente y ejecutarse de acuerdo con las necesidades de cada organización. Si bien se pueden encontrar las medidas específicas recomendadas para cada fase en los modelos presentados, este apartado persigue el objetivo de exhibir las contramedidas generales que muestran una mayor relación con las debilidades explotadas por los atacantes.

La herramienta fundacional es el documento que declara la "Política de Seguridad Informática" y debe expresar claramente la visión de la organización respecto a la seguridad con el aval de la máxima autoridad. De ella desprenden luego los documentos necesarios, como normas, procedimientos, estándares técnicos, etc., que contienen los detalles para poder cumplir con las expectativas expresadas en la política general. Si bien dentro del marco regulatorio de cada actividad particular, en algunos casos, rigen normas de cumplimiento mínimo y obligatorio respecto a la ciberseguridad, el estándar dictado y actualizado en forma permanente de la familia normativa 27.000 de la Organización Internacional de

Estándares (ISO) en conjunto con la Comisión Electrotécnica Internacional (IEC), es un marco adecuado para atender las necesidades de las organizaciones de todas las escalas, siendo además la referencia de la cual derivan las regulaciones y recomendaciones del ámbito de la logística, como por ejemplo las recomendaciones de la Organización Marítima Internacional que entraron en vigor el 1ero de enero del 2021.

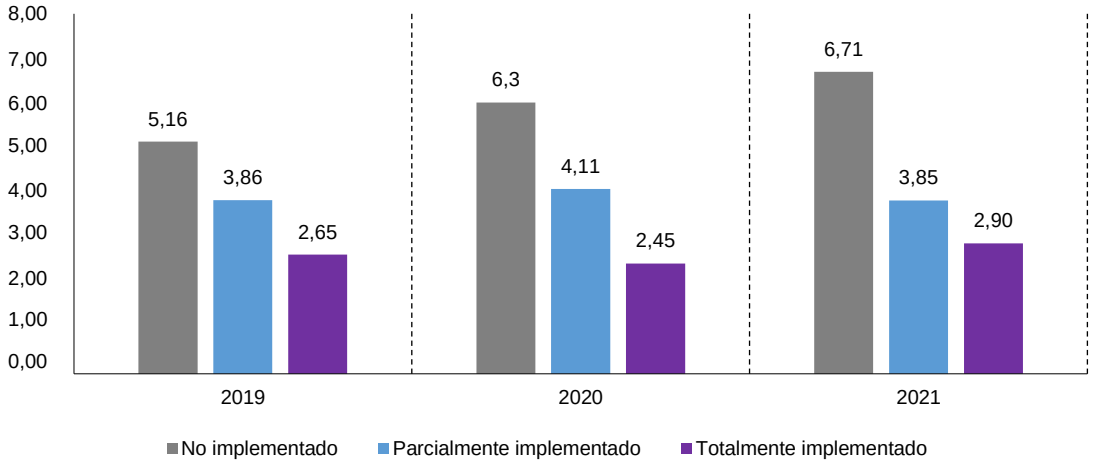
Comprendida la importancia de un plan rector para llevar adelante las tareas que pueden reducir el riesgo frente a los incidentes de ciberseguridad, se enumeran a continuación aquellas contramedidas que se han destacado desde el punto de vista de la resiliencia cibernética, o en algunos casos la ausencia de estas que derivaron en mayores costos o tiempos para volver a la normalidad la actividad luego de haber sufrido un incidente.

Como se ha anticipado en el apartado anterior, la medida que más ha ayudado a las organizaciones al momento de enfrentar una crisis provocada por un ciberataque, y que además puede cubrir otro tipo de situaciones inesperadas, es contar con un Plan de Recuperación ante Desastres o Disaster Recovery Plan (DRP), como pieza clave del BCP; este debe estar, por supuesto redactado, aprobado, debidamente comunicado y disponible en los medios para ser utilizado oportunamente, pero más importante aún, debe ser dinámico y los integrantes de la organización involucrados con los roles claves, liderar la tarea de realizar pruebas periódicas con el convencimiento de que esta práctica es el mejor aliado para el momento en que la crisis se produzca. Esto evitará la improvisación y aumentará la confianza en las acciones que el equipo deberá desempeñar en el momento indicado. De la misma manera que un atleta se prepara durante muchos años y pasa por instancias que van elevando su nivel de exigencia para lograr su mejor versión en una competencia de alto rendimiento, el equipo de respuestas del DRP debe proceder con las actividades operativas que darán a la organización su mejor versión en un momento crítico. Desafortunadamente, como se ha mencionado previamente, en el estudio realizado por CEPAL en la región de América Latina y el Caribe, donde se encuestó a organizaciones de diverso tamaño integrantes de la cadena logística, se ha encontrado que solo el 37% de las mismas cuentan con un DRP y solo el 22% realizan pruebas periódicas del mismo, lo cual presenta una importante oportunidad de mejora que debería acompañar los esfuerzos que se realicen en la región en el camino de la transformación hacia una logística inteligente.

El siguiente factor determinante cuando un incidente ha ocurrido es la certeza de mantener las redes operativas correctamente separadas de las administrativas o tradicionales de TI. Algo sencillo de expresar pero muy difícil de satisfacer en entornos que nacieron aislados como las redes de gestión operativa, o piso de planta, y en la actualidad se les exige prestaciones similares a los entornos de TI, desde la necesidad de obtener información en línea para una correcta decisión operativa, hasta el soporte remoto de proveedores especializados de manera inmediata. Sin embargo, a la hora de desencadenarse un ataque, el movimiento lateral del vector malicioso hacia las redes operativas puede llegar a afectar funciones que no puedan continuarse de manera manual o escalar a situaciones de caos inesperadas. Citando nuevamente el evento de Colonial Pipeline descripto en el apartado de incidentes ocurridos, algunos operadores de infraestructura crítica dicen que instalar tales puertas de enlace unidireccionales a lo largo de una instalación de la magnitud de la analizada, puede ser complicado o prohibitivamente costoso, sin embargo, el costo de implementar esas salvaguardas sigue siendo más económico que las pérdidas causadas por el tiempo de inactividad de un incidente.

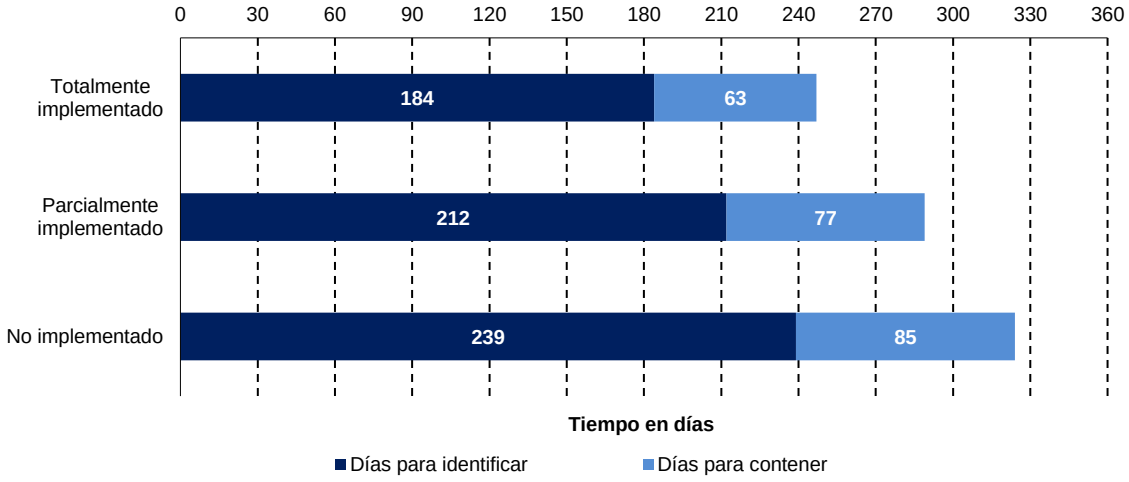
Si bien las medidas mencionadas son de gran utilidad en el caso que se desate un incidente, retomando los modelos ATT&CK y CKC7, los mecanismos de defensa y control correspondientes a las primeras fases pueden detectar y frenar a tiempo un ataque. Las organizaciones que cuentan con la implementación de sistemas de monitoreo inteligente siguiendo el concepto de ciberinmunidad, han logrado reducir a 247 días el tiempo para detectar y contener una brecha de seguridad, lo cual significa 42 días por debajo del promedio, reduciendo al mismo tiempo los costos totales de las mismas a 2.9 millones de dólares ubicándose 3.8 millones por debajo de los más elevados y 1 millón de dólares debajo del promedio (IBM Inc., 2021).

Gráfico 6
Costo promedio de una brecha de seguridad por nivel de automatización implementado
(Costo en millones de USD)



Fuente: Elaboración propia basada en datos de IBM Inc.

Gráfico 7
Tiempo promedio para identificar y contener una brecha de seguridad por nivel de automatización



Fuente: Elaboración propia basada en datos de IBM Inc.

Al mismo tiempo, como se ha señalado en la sección I.C.2, la técnica de evasión de la defensa se utiliza en un porcentaje bajo de los ataques, por lo cual la implementación de una detección en tiempo real con alertas pertinentes resulta muy efectiva en el contexto actual.

Una contramedida que es fundamental para reducir la superficie de ataque y que, junto con la mencionada se debe realizar un adecuado respaldo de información y contar con antivirus correctamente actualizado, se consideran necesidades básicas a cubrir, mantener el *software* de las instalaciones con versiones vigentes y con las actualizaciones disponibles implementadas. Previamente se explicó la dificultad que esta actividad presenta en las dinámicas de las organizaciones, pero la amplia disponibilidad de herramientas que permiten la automatización de esta

tarea resuelve sin mayores inconvenientes esta dificultad si se entiende que su importancia es ni más ni menos que el 30% de la superficie de ataque. Es necesario considerar la actividad de actualización del *software* de base como un mantenimiento preventivo absolutamente asociado al equipo en servicio. Se podría considerar similar a los mantenimientos mecánicos de cambios de lubricante periódicos que se le realizan a un vehículo. Pasados el período determinado por el tipo de motor y de lubricante, el daño al motor sería inminente sin el recambio necesario. La correcta planificación de esta actividad involucra agrupar a los activos de manera que cada grupo puede recibir una definición de frecuencia de actualización adecuada con las funciones y criticidad asignada. Se debe tener presente que según Coveware, como se presentó en la sección donde se explica el modelo ATT&CK, el movimiento lateral se utiliza en todos los ataques, por lo cual es importante mantener un criterio de actualización homogéneo para la totalidad de los equipos, ya que las computadoras instaladas en la red pueden ser vulneradas por falta de instalación de actualizaciones, independientemente de la función que cumplen y que una vez vulneradas pueden transformarse en la base para el movimiento lateral.

De manera similar al *software*, ocurre con las actualizaciones del *hardware*, pero con una complejidad para su reemplazo por caducidad mucho mayor que el *software*. Si bien es menos frecuente por tratarse de productos donde es más difícil conseguir información que para el *software*, existen muchos casos de ataques correspondientes a vulnerabilidades del *hardware*. Es recomendable considerar desde la adquisición del equipamiento, el costo total del producto y su amortización en relación con el ciclo de vida anunciado por el fabricante, considerando que finalizado el mismo, es necesario su reemplazo.

Se ha esbozado en las vulnerabilidades explotadas, que el factor humano está directamente relacionado con el 60% de las causas de los ataques, lo cual es resultado del formato cibernético de los artilugios y técnicas utilizados desde el principio de todos los tiempos; esto es, explotar las debilidades o distracciones de los seres humanos a través de la psicología que, en muchos casos, representa un nivel de dificultad bajo en comparación con debilitar barreras tecnológicas sofisticadas. Por este motivo**, la concientización permanente de las personas en materia de ciberseguridad es una contramedida imprescindible** que debe acompañar el resto de las acciones tecnológicas. Naturalmente cuanta más automatización exista en los procesos, menor es la incidencia del factor humano en los incidentes de seguridad.

Esto no significa que un equipo de personas altamente capacitadas y concientizadas en ciberseguridad asegure que no vayan a existir incidentes o ataques, pero lo contrario, es decir que aparezcan incidentes en un ambiente donde las personas nos conozcan sobre la problemática casi podría darse por asegurado.

Dado el objetivo de este documento, el desarrollo de conocimiento sobre la materia y la generación de conciencia individual y colectiva es una actividad que debería desarrollarse en los ámbitos institucionales internacionales, regionales y nacionales, tanto en las instituciones públicas como en las privadas; sobre este aspecto se amplía información en los apartados II.B.3. y II.B.4.

B. Aspectos de seguridad de las principales tecnologías implementadas en *Smart Logistics:* fortalezas y debilidades

Las tecnologías que se presentan en esta sección no son tecnologías que trabajen en forma independiente, sino que, todo lo contrario, el desarrollo actual que tienen las mismas es posible gracias a la otra ya que se complementan, lo que genera un círculo virtuoso respecto a las capacidades que las mismas tienen o pueden tener. Por lo tanto, la aparición de un virus, las equivocaciones humanas, los sabotajes, las vulnerabilidades informáticas y los ciberataques dirigidos pueden afectar a una o varias de estas tecnologías, lo cual hace que ese círculo virtuoso que se menciona también sea el talón de Aquiles de estas. Es por este motivo que, como se menciona en sendas oportunidades a lo largo del documento, la seguridad tiene que ser abordada de una forma integral, no solo desde el punto de vista de la tecnología en sí, sino de todo el conjunto o sistema que hace posible su funcionamiento.

1. *Internet of Things*

La internet de las cosas (*IoT*) es un conjunto de diversas tecnologías que evolucionan y se difunden con rapidez, y que interactúan con el mundo físico combinando la informática tradicional (IT) con la tecnología operativa como ser sensores o chips.

La principal ventaja que da la irrupción de la tecnología *IoT* es, por un lado, proporcionarles a los objetos funcionalidades de informática, almacenamiento y conectividad para así aumentar sus capacidades y funcionalidades, como ser el acceso remoto para ver el estado de un dispositivo, realizar cambios en la configuración, darle instrucciones. Pero también le permite, a través de la aplicación de otras tecnologías que se tratan en el presente documento (Conectividad 5G, *Big Data*, Inteligencia Artificial, etc.), la capacidad de proporcionarle datos del mundo físico para que otros sistemas utilicen los mismos para la toma de decisiones o prever eventos futuros.

En lo que respecta a la seguridad, es pertinente mencionar que los mismos riesgos que tenemos presentes en los sistemas informáticos tradicionales (TI) también están presentes en los dispositivos *IoT*.

La facilidad con la que los dispositivos *IoT* se conectan con el mundo físico hace que los riesgos de ciberseguridad y privacidad se vean afectados, ya sea a través de la manipulación de sensores de manera que se puede influir en el comportamiento o toma de decisión, o de los datos que estos dispositivos dicen acerca de las personas u otros dispositivos.

Otro factor para tener en cuenta es la forma en que los dispositivos *IoT* se gestionan, ya que muchos de estos actúan como bloques de los cuales se cuenta con poca o ninguna visibilidad de su estado y composición, incluida la identidad de los servicios o sistemas externos con los que interactúan, y poco o ningún acceso a su *software* y configuración, o a la gestión de estos.

Además, existen una serie de riesgos tecnológicos que pueden asociarse a los dispositivos *IoT*:

- falta de capacidad de gestión y administración de dispositivos (centralización de la gestión de los dispositivos y de la seguridad),
- falta de monitoreo de dispositivos a través de logs sobre el funcionamiento,
- interfaces con el usuario limitadas,
- amplia variedad de *software*, del cual mayormente no conocemos como está desarrollado o si tiene fallas conocidas que no puedan ser remediadas,

- falta de actualizaciones de seguridad o actualizaciones del *sofware* embebido, y a menudo si las hay se pone en compromiso la funcionalidad del dispositivo y la integración con otros sistemas,
- documentación técnica ausente o limitada,
- ciclo de vida corto de los dispositivos,
- falta de herramienta de inventariado de dispositivos,
- numerosos intervinientes para un mismo servicio (fabricante de *hardware*, *software*, proveedor de telecomunicaciones, proveedor de nube) (NIST, 2019).

Dada la creciente importancia del uso de *IoT* y sus riesgos asociados, la Organización Internacional para Estándares está desarrollando la norma ISO/IEC 27400, actualmente en borrador, específica para dar tratamiento a los riesgos de ciberseguridad del ecosistema de *IoT* (ISO/IEC, 2021).

Se puede concluir respecto a *IoT* que es una tecnología que está presente para ser utilizada en muchos dispositivos de manera muy sencilla, pero también en muchos casos con un alto nivel de incertidumbre en lo que respecta a su impacto en la seguridad en la red a la que se conecte. Por lo tanto, se recomienda analizar el impacto de cada uno de los aspectos mencionados en la organización, o ecosistemas de organizaciones, durante el proceso de adopción de este tipo de tecnología.

2. Comunicaciones 5G

La tecnología 5G resulta vital para la interconexión de una gran variedad de dispositivos *IoT* entre sí y también con el mundo IT a través de lo que se denomina el Edge Computing. Las ventajas de las comunicaciones 5G no solo tratan acerca de la velocidad de conexión (que por cierto es muy superior al 4G), sino por sobre todo por la capacidad que la tecnología tiene para conectar la gran cantidad de dispositivos de forma simultánea y además proporcionar una baja latencia que es un elemento central para el desarrollo de funcionalidades en tiempo real (Terol, 2021).

Esta tecnología también presenta varios desafíos en materia de ciberseguridad que tienen que ser tratados antes de su masificación. Algunos de ellos tienen que ver con la tecnología en sí, y otros con los dispositivos que van a utilizarla:

- **Seguridad descentralizada**. Las redes previas a la 5G tenían menos puntos de contacto de tráfico de *hardware*, lo cual facilitaba los controles de seguridad y el mantenimiento. Los sistemas dinámicos basados en *software* de 5G tienen muchos más puntos de enrutamiento de tráfico. Para estar completamente seguros, todos estos necesitan supervisión. Como esta tarea podría resultar difícil, si no se asegura su ejecución de podrís derivar en un área no segura que podría comprometer otras partes de la red.
- **Un ancho de banda mayor pondrá a prueba la supervisión de seguridad actual**. Si bien las redes actuales están limitadas en cuanto a velocidad y capacidad, esto ha ayudado a los proveedores a supervisar la seguridad en tiempo real. Por lo tanto, los beneficios nativos de una red de tipo 5G podrían atentar contra la ciberseguridad. La velocidad y el volumen de datos añadidos se transformarán en un desafío para los equipos de seguridad, donde deberán crear nuevos métodos para detener las amenazas.
- **Muchos dispositivos de *IoT* se fabrican con carencias en materia de seguridad**. Como se ha mencionado en la sección específica de esta tecnología, no todos los fabricantes dan prioridad a la ciberseguridad, como se ve en muchos dispositivos inteligentes de baja gama. La red 5G significa más utilidad y potencial para la *IoT*. A medida que se fomenta la conexión de más dispositivos, los miles de millones de dispositivos con diversos niveles de seguridad significan miles de millones de posibles puntos de brechas de seguridad. Los televisores

inteligentes, cerraduras de puertas, frigoríficos, altavoces e incluso dispositivos secundarios como un termómetro para pecera pueden constituir un punto débil de la red. La falta de estandarización de seguridad en los dispositivos de *IoT* podrían significar brechas en una red a través de las cuales la ciberdelincuencia podría obtener acceso con más facilidad que en los dispositivos tradicionales de TI.

- **La falta de cifrado al principio del proceso de conexión revela información del dispositivo que puede usarse para ataques dirigidos**. Esta información ayuda a los intrusos a saber exactamente qué dispositivos están conectados a la red. Los datos como el sistema operativo y el tipo de dispositivo (teléfono inteligente, módem de vehículo, etc.) presentan una debilidad que los atacantes pueden explotar durante la etapa de descubrimiento (Kaspersky Lab., 2021).

Se deberá observar cuidadosamente la evolución de las redes 5G y considerar en el presente las medidas adicionales que deberán implementarse en caso de ser el medio de conexión utilizado, ya que, si bien las velocidades que proveen las redes de 5ta generación en la actualidad posibilitan y auguran grandes transformaciones en los procesos logísticos, la seguridad sigue teniendo puntos de atención.

3. Robótica y automatización

Los avances en la robótica y en la automatización de procesos están revolucionando todo tipo de industria, principalmente las relacionadas con la manufactura y logística, logrando una elevada eficiencia en los procesos; pero también presentan una serie de desafíos que no existían. Actualmente, la integración entre los sistemas de control industriales y los sistemas de gestión es relativamente elevada, lo cual presenta una serie de desafíos que deben abordarse, ya que los riesgos asociados a estos sistemas pueden generar un gran impacto, como se ha observado, por ejemplo, en el caso presentado de Colonial Pipeline. Estos problemas asociados a la ciberseguridad tienen su origen, principalmente, en que los sistemas de control permanecieron aislados durante mucho tiempo, existiendo una barrera física para poder acceder a los mismos. Al flexibilizar el acceso a ellos, han expuesto las debilidades que presenta los sistemas tradicionales de TI, como ser:

- vulnerabilidades no descubiertas o que aún no se han publicado parches,
- incorrecta asignación de permisos de accesos,
- errores en la configuración,
- utilización de componentes cerrados o PC embebidas que no tienen sistemas discontinuados.

Desde el punto de vista de la ciberseguridad, para la robótica y las redes de automatización, se recomienda cumplir estrictamente el aislamiento de las redes de control, de manera que el tráfico permitido sea unidireccional desde dentro de ellas hacia el exterior del perímetro y nunca en sentido inverso. Para el uso en sistemas de infraestructura crítica, existen dispositivos que realizan el enlace por medio de transmisores ópticos en la red de automatismos con sus correspondientes receptores en la red de TI, de manera que, por restricción de diseño, el tráfico de datos puede ir solo en una dirección (Ginter, 2013). Otra sugerencia es utilizar en las redes de automatismos, siempre que sea posible, soluciones que implementen tecnologías que cuenten con estándares abiertos, similares a los de TI ya que la experiencia y los dispositivos que trabajan con este tipo de comunicaciones, llevan muchos años evolucionando sobre la seguridad debido a la exposición a la que se han sometido durante su ciclo de vida.

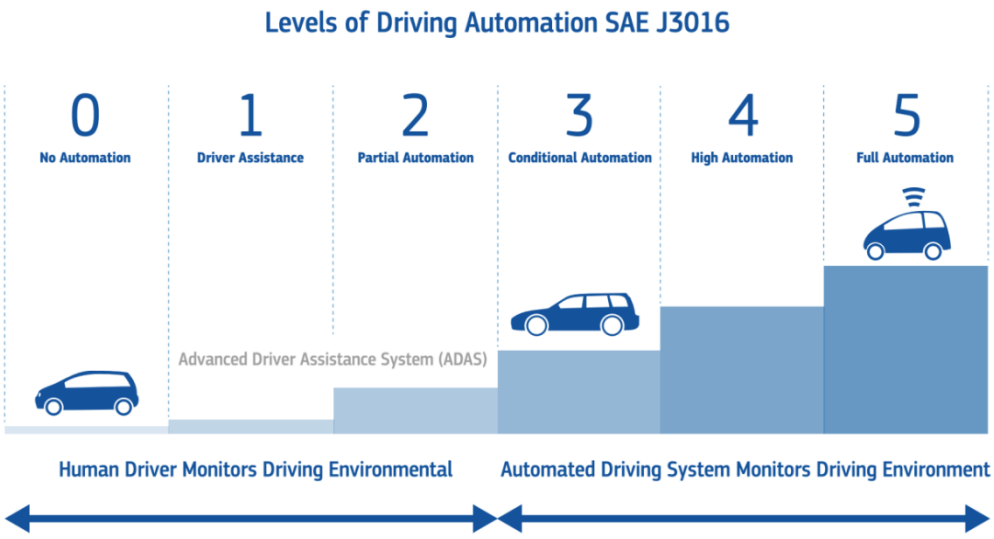
4. Vehículos autónomos

El avance de los vehículos autónomos se da gracias a la aparición y desarrollo de varias tecnologías tratadas en este documento (*IoT*, Comunicaciones, *Big Data*, Inteligencia Artificial) que se complementan para lograr una autonomía parcial o total, en los casos más avanzados. Las

limitaciones para la conducción autónoma no se dan por la tecnología sino por la desconfianza que aún existe en las personas acerca de esta tecnología y a la carencia de un marco regulatorio apropiado.

Existen en la actualidad distintos niveles de autonomía, que independientemente de su estadio, sus fortalezas o debilidades se pueden ver potenciadas o atenuadas.

Diagrama 3
Levels of Driving Automation SAE J3016



Fuente: SAE J3016B: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles'. 2018.

Un factor importante, además de la conducción de un vehículo en forma autónoma, es entender cómo se comunica el mismo con otros vehículos y el entorno, ya que dependiendo del grado de integración que estos tengan, se puede aumentar la eficiencia:

- **Vehicle-to-Network (V2N)**: permite la conexión del vehículo con internet para intercambiar datos en tiempo real de rutas, estado del tráfico, clima, reportes de trabajos o accidentes.
- **Vehicle-to-Vehicle (V2V)**: conecta a vehículos cercanos que están compartiendo una misma ruta, intercambiando información de ruta, posición, estados de frenos, por ejemplo.
- **Vehicle-to-Infrastructure (V2I) and Infrastructure-to-Vehicle (I2V)**: refiere a la comunicación que puede existir entre un vehículo y una barrera, o un semáforo.
- **Vehicle-to-Person (V2P)**: es la comunicación entre los vehículos y dispositivos de uso personal, como ser un Smartphone o un dispositivo conectado (*wearables*) que pueden utilizar ciclistas, peatones, por ejemplo.
- **Vehicle-to-Device (V2D)**: refiere a la conexión que puede existir entre un vehículo y cualquier dispositivo *IoT* cercano que está conectado a internet.

Estas capacidades de comunicación hacen que los vehículos autónomos no solo funcionen gracias la inteligencia que tiene el vehículo en si solamente para poder detectar lo que sucede en el entorno y tomar acciones, sino que también se puedan nutrir de un volumen muy importante de datos proveniente de otros actores para aumentar la seguridad de la conducción.

Naturalmente el desarrollo de vehículos autónomos presenta una gran oportunidad para la logística y se encuentra muy desarrollado en el uso de drones en la última milla de las entregas. Además, en base a los avances tecnológicos actuales, se proyectan para la próxima década la automatización de los medios más habituales como buques, trenes, camiones, etc.; pero como el objetivo del presente documento no es el desarrollo propio de la tecnología, no se ahondará en cada uno de ellos.

Considerando que para la conducción autónoma se combinan varias tecnologías abordadas en detalle a lo largo de la presente sección, las consideraciones extra que se suman a ellos son el cambio en la superficie de ataque a la que se está expuesto, ya que se trata de un blanco en movimiento, y también el impacto que un incidente puede tener, pudiendo considerarse desde la pérdida de la privacidad hasta el secuestro de un vehículo por parte de un atacante.

El cambio paradigmático de la conducción vehicular autónoma mediante el uso de la tecnología presenta un desafío mayor que guarda relación con los aspectos legales y éticos de esta, lo cual hace necesaria una legislación clara; no solo la adecuación del marco jurídico interno de cada país, sino también a nivel regional e internacional. Algunos interrogantes que se presentan en la actualidad, sobre los cuales se deberá seguir investigando, son los siguientes:

- ¿qué sucederá con las aseguradoras y las legislaciones vigentes en esta materia?,
- ¿quién será el responsable de las acciones llevadas a cabo por vehículos autónomos?,
- ¿al momento en que no sea evitable un accidente, que criterios tomará un vehículo para determinar contra que chocar? (ENISA, 2021).

La resolución urgente de estos interrogantes es necesaria para poder establecer normas claras y posibilitar la puesta en servicio de los vehículos autónomos cuando estén listos para salir a producción y necesiten atravesar fronteras regionales, o atravesar aguas o espacio aéreo internacional.

5. *Blockchain*

En el estudio realizado por CEPAL por Álvarez y Sánchez, 2021, se ha mencionado que la utilización de *blockchain* podría traer a las Ventanillas Únicas de Comercio Electrónico (VUCE) y a los Port Comunity Systems (PCS) ventajas como aumento de la interoperabilidad, mejora de la trazabilidad, automatización de procesos y aumento en la confiabilidad de los datos.

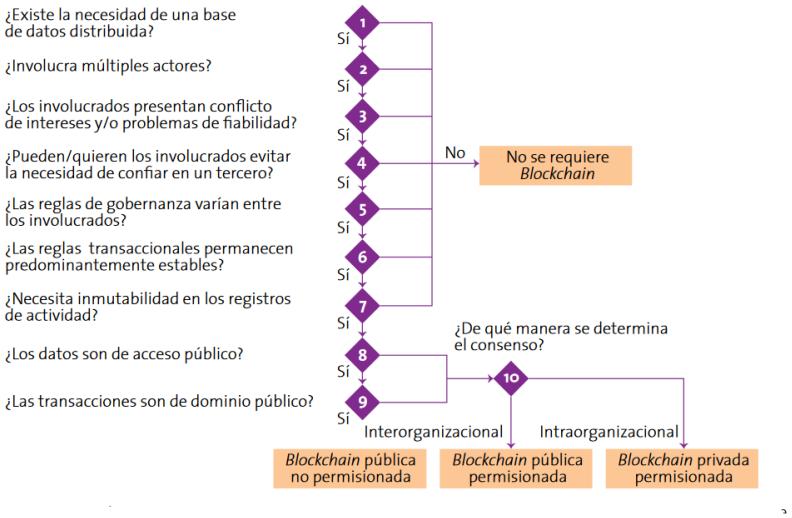
Desde el punto de vista de la seguridad, *blockchain* presenta características intrínsecas en su diseño relacionadas con la inmutabilidad de los datos y la resiliencia del sistema, que le confieren, con un correcto diseño de confidencialidad, la capacidad de responder naturalmente a los conceptos de disponibilidad e integridad de la información administrada. Tanto es así que luego del evento de *ransomware* sufrido en el año 2017, fue la firma MAERSK misma quien desarrollo una plataforma basada en *blockchain*, denominada Tradelens, con la finalidad obtener los beneficios que presenta la gestión de la información relacionada con la carga en un entorno que mejore la resiliencia de los datos.

La inmutabilidad de los datos en esta tecnología está asegurada por la forma en la que se relaciona un bloque con el siguiente, y la resiliencia de la red está dada porque para confirmar una transacción, es necesario contar con el consenso de la red, que viene dado por la mitad más uno de los nodos que la compongan, de manera que si una parte de esa red no estuviera disponible por cualquier tipo de incidente, el resto de los nodos seguirían operando y el sistema podría dar servicios de manera ininterrumpida.

El estudio realizado por Díaz, Valdés y Pérez también de CEPAL (CEPAL, 2021), específicamente sobre *blockchain* por el interés que esta tecnología clave de la industria 4.0 despierta para la logística internacional, desarrolla el potencial de la cadena de bloques para la determinación de procedencia y origen de los productos, optimización de las operaciones comerciales, intercambio seguro de información, automatización de procesos de contratos y pagos comerciales, y presenta una serie de

pasos básicos, los cuales se exhiben a continuación, que permiten evaluar si *blockchain* es la tecnología adecuada para ser utilizada en una necesidad determinada:

Diagrama 4
Árbol de decisión para el uso de *blockchain*



Fuente: Elaboración propia sobre la base de A. B., Pedersen, M. Risius and R. Beck, "A Ten-Step Decision Path to Determine When to Use *Blokchain* Technologies,"MIS Quarterly Executive: Vol. 18: Iss. 2, article 3 [en línea] https://aisel.aisnet.org/misqe/vol18/iss2/3.

En LAC se encuentra en marcha el proyecto CADENA que atiene al Servicio Nacional de Aduanas Chile, la Dirección de Impuestos y Aduanas Nacionales de Colombia, la Dirección General de Aduanas de Costa Rica, el Servicio de Administración Tributario de México, la Superintendencia Nacional de Administración Aduanera y Tributaria de Perú, la Superintendencia de Administración Tributaria de Guatemala (SAT), el Servicio Nacional de Aduana del Ecuador (SENAE) y la Aduana Nacional de Bolivia, por lo cual representa una importante oportunidad de desarrollo para la logística inteligente con seguridad integrada desde el diseño, que si bien en la actualidad resuelve específicamente la problemática de una VUCE, sobre la cual se podría analizar la integración a una solución vaya incorporando otros módulos que permitan extender el alcance hacia los extremos de la cadena logística.

6. *Big Data*

La voracidad por aumentar la cantidad de fuentes de datos para que las mismas se analicen íntegramente y se pueda llegar a obtener información precisa y en tiempo real, reviste un riesgo a la hora de seleccionar que tipo de datos se va a incorporar al modelo en estudio. Hoy existe una fuente casi inagotable de datos y metadatos para analizar (sobre todo que se suman a las fuentes de datos tradicionales, una variedad muy grande de sensores provenientes del IoT, por ejemplo) que presentan la dificultad de distinguir y no pasar los límites legales y éticos acerca del uso de la información (Telefónica Tech, 2021).

Los principales aspectos de seguridad de *Big Data*[5] no vienen por el lado de la robustez de la tecnología que lo hace posible, sino de las aplicaciones que hacen uso de este para el servicio de la seguridad de las organizaciones denominados Gestión de Eventos e Información de Seguridad o *Security Information and Event Management (SIEM)*. Los sistemas SIEM, como por ejemplo IBM QRadar o Splunk, se valen de la recolección de datos desestructurados provenientes de todos los sistemas de una organización para realizar análisis complejos (mediante algoritmos de ML e IA) de toda la información disponible en tiempo real para poder detectar amenazas o comportamientos anómalos. El análisis de información desestructurada proveniente de múltiples fuentes de datos y la correlación que existe los diversos eventos enumerados por ellas, es una tarea que excede el campo de los seres humanos, tanto por el volumen de la información, como también por el tiempo que lleva ejecutar dichos análisis, cuestión central a la hora de detectar un ataque. Los sistemas SIEM constituyen uno de los elementos fundamentales de los sistemas de ciberinmunidad.

La recolección de datos en gran escala permite analizar eventos pasados y ayuda a identificar el origen de los ataques o bien el comportamiento que tuvieron los sistemas antes de que el mismo se haya ejecutado para poder realizar modelos de análisis predictivos que utilizan los SIEM para ir mejorando y manteniéndose actualizados. Por ellos es de vital importancia no solo contar con sistemas que tengan esta capacidad de análisis de información, sino también de cómo se van a alimentar los mismos (ENISA, 2016).

Los riesgos asociados a la tecnología del *Big Data*, en la mayor parte de los casos, guardan relación o son una consecuencia de sus propias virtudes. Al ser una fuente que tiene mucha información relevante, los sistemas de *Big Data* son un objetivo muy codiciado para cualquier atacante.

El aspecto de la seguridad donde debe prestarse especial atención en los sistemas de *Big Data* es el control de acceso, ya que un acceso indebido podría poner en duda la veracidad de los datos afectando negativamente el modelo de datos y entregando información errónea. Además, quien cuente con acceso a estos sistemas será capaz de tener una visión absoluta de la información, lo que supone también un desafío desde el punto de vista de la confidencialidad y privacidad de los datos.

7. Inteligencia Artificial

De la misma manera que ocurre en otro tipo de actividades, la inteligencia artificial está transformando la forma de abordar las complejidades de cada disciplina, convirtiendo las soluciones mediante la asistencia de la computadora para resolver las tareas repetitivas, dejando para los humanos la creatividad y la intuición. El gráfico a continuación muestra un listado de actividades transversales a todas las disciplinas, donde puede apreciarse cuales actividades se consideran en la actualidad exclusivas del terreno humano y cuáles del terreno computacional. En el centro se expresan aquellas que presentan una situación híbrida con mayor o menor participación de cada uno de ellos, distinguiéndose las actividades donde el ser humano valida y sostiene el resultado obtenido por las máquinas, de aquellas donde la capacidad de procesamiento de la máquina amplifica las actividades humanas.

[5] Al *Big Data* frecuentemente se le caracteriza a través de la célebre definición de las tres 'V'3: Volumen, Variedad y Velocidad. Esto es, manejar un gran volumen de información (en relación con la cantidad), procesar los datos a gran velocidad o en tiempo real (rapidez en la obtención de resultados interpretativos) e integrar gran variedad de fuentes de información para, a través de diferentes técnicas analíticas, generar conocimiento y valor – Fuente: Telefónica Tech - https://empresas.blogthinkbig.com/informe-covergencia-iot-big-data-ia/.

Cuadro 2
IA - Distribución de las tareas entre humanos y computadoras

Liderar	Empatizar	Crear	Juzgar	Entrenar	Explicar	Sustentar	Amplificar	Interactuar	Personalizar	Transaccionar	Iterar	Predecir	Adaptar
Humanos				Los Humanos complementan a las máquinas			La IA amplifica el poder humano				Computadoras		
				Actividades Híbridas Humanos+ Computadoras									

Fuente: Elaboración propia en base a datos de Daugherty, P. R., & Wilson, H. J. (2018). Human + machine: Reimagining York in tue agüe os AI. Boston, Massachusetts: Harvard Business Review Press.

Al hablar de fortalezas y debilidades relacionados a la inteligencia artificial, los aspectos de seguridad intrínsecos son similares a los desarrollados para el *Big Data*. Sin embargo, la IA presenta una particular necesidad de atención en el proceso de autoaprendizaje que se realiza mediante datos de entrenamiento para la toma de decisiones. Mayoritariamente, la IA trabaja como un sistema cerrado del cual se tiene poco conocimiento de su funcionamiento interno, y posee un comportamiento autónomo, lo cual dificulta las tareas de revisión para verificar el criterio de las decisiones a tomar, por lo tanto, se requiere una cuidadosa planificación y monitoreo del proceso de aprendizaje. Luego se debe contar con controles de auditoría periódicos similares a los procesos realizados por los humanos, que sirvan de retroalimentación y mejora continua. Es decir que un proceso asignado a la inteligencia artificial requiere similar tratamiento de gestión a los realizados por los humanos, considerando particularmente el volumen e impacto de las decisiones que toma el sistema analizado.

En otras palabras, el principal riesgo que reviste la inteligencia artificial es el que resume el creador de internet Sir Tim Berners-Lee postulando que la inteligencia artificial podría comprender negocios impulsados por decisiones tomadas por algoritmos sin la participación humana, a medida que aumenten los datos y su disponibilidad (Mceleny, 2015).

La gestión de la actividad de ciberseguridad no es una excepción al resto de las actividades y está atravesando el mismo proceso de transformación, razón por la que se hará referencia al uso de la inteligencia artificial para la defensa reactiva o proactiva de las infraestructuras y sistemas de información, entendiendo también que las mismas características pueden ser explotadas para hacer el mal; actualmente, la Inteligencia Artificial se tornó un factor crucial para los sistemas de protección contra ciberataques ya que, valiéndose de ella, se pueden analizar una gran cantidad de datos en tiempo real, realizar correlación de eventos y determinar cuándo se presenta una amenaza, o se está atravesando los inicios de un ataque, dotando al sistema de la capacidad para ejecutar una medida proactiva, reactiva o defensiva de manera automática, concepto que se ha desarrollado como ciberinmunidad. Desafortunadamente, actualmente también se aplica el concepto de inteligencia artificial para refinar virus informáticos, y para que los *malwares* o *ransomwares* aprendan automáticamente a saltear las nuevas medidas de protección de las herramientas de seguridad, por lo cual aquellos que prescindan de esta herramienta para la defensa, presentarán una desventaja importante durante todo el ciclo de vida de un ataque.

Se puede concluir que, a diferencia de los sistemas transaccionales, la Inteligencia Artificial debe ser controlada en la toma de decisión del mismo modo que los procesos realizados por humanos, y constituye una pieza central para el presente y futuro de la ciberdefensa.

8. Realidad aumentada y realidad virtual

Si bien están íntimamente relacionadas, debe diferenciar a la realidad aumentada (RA) de la realidad virtual (RV); la primera supone un enriquecimiento del mundo real agregando elementos digitales y datos, mientras que la realidad virtual crea un entorno digital. La confusión sobre ambas tecnologías se puede dar porque la interfaz utilizada en ocasiones puede ser la misma o asemejarse.

Cuando se habla de riesgos, existe un elemento común a ambas tecnologías que es la privacidad, ya que más allá de la experiencia del uso de la tecnología, las mismas son capaces de recopilar todo lo que se ve y se hace mientras se las utiliza.

Además de las preocupaciones por la privacidad, los dispositivos AR y VR están conectados a la red como cualquier otro ordenador o smartphone, formando parte de IoT y, como cualquier dispositivo conectado, manejan la transmisión y el almacenamiento de datos, del que los ciberdelincuentes buscan tomar control. Cuando se trata de las experiencias inmersivas esto tiene un potencial especialmente preocupante en el espionaje corporativo y la ingeniería social. En los casos donde la tecnología puede llegar al punto de convencer al cerebro de que este, está en algún lugar donde no lo está, se potencian aún más (Isotopy, 2021)

La eficiencia y eficacia con la cual se están transformando los procedimientos, por ejemplo de mantenimientos complejos o de navegación vehicular terrestre y naval, mediante la ayuda en vivo de la realidad aumentada, y las capacitaciones masivas o entrenamientos especiales, como por ejemplo fuerzas especiales, brigadas de emergencias, modeladas en realidad virtual, están transformando el uso de la tecnología llevándola al uso corporativo, por lo tanto se debería poner especial atención en la información de imágenes y espacios sensibles que la tecnología utilice, determinando un adecuado control de acceso que asegure su confidencialidad.

El desarrollo de estas tecnologías (sobre todo de la realidad virtual), ha contribuido al desarrollo y refinamiento de lo que se denomina actualmente como *Deep Fakes*, que consiste en la manipulación de archivos multimedia y el principal riesgo que existe es la manipulación de las personas para lograr un objetivo propio (Jackson, 2020).

9. Impresión 3D

La impresión 3D está cambiando los procesos productivos alrededor del mundo, y podrían ser utilizadas para disminuir distancias y tiempos en diferentes cadenas de valor, como por ejemplo en los proveedores de autopartes dentro de la industria automotriz.

La tecnología en si también está evolucionando constantemente lo cual está generando una nueva industria en sí. No tanto tiempo atrás, las primeras impresoras 3D solo eran capaces de crear objetos plásticos y de tamaños acotados. Actualmente se ha avanzado no solo en el tipo de materiales que pueden ser "impresos" (metales, compuestos, materiales biológicos), sino también en la precisión que se puede lograr con estos equipos. Con ello también se va abriendo un nuevo abanico de aplicabilidades que puedan tener.

He aquí algunas de las principales fortalezas que posee esta tecnología:

- Versatilidad. La revolución que supone para la manufactura de productos. Una sola impresora 3D es capaz de realizar infinidad de productos distintos.
- Flexibilidad y prototipado rápido. El límite es la imaginación y la capacidad para representar las ideas en 3D y luego fácilmente obtener el prototipo del producto.
- Reducción de costos. Tanto en el proceso de producción cómo en el proceso de transporte.

- Personalización. Una de las ventajas más atractivas, es la posibilidad de realizar prendas, objetos de todo tipo y productos de forma personalizada y exclusiva.
- Una nueva industria y un nuevo sector que creará nuevos puestos de trabajo y nuevas formas de negocio.
- Aplicaciones múltiples según el campo de aplicación. Por ejemplo, en medicina encontramos la creación de prótesis o incluso la impresión de tejidos orgánicos.

Como ocurre con toda tecnología donde hay un cambio de paradigma, y se ha marcado repetidamente en el presente estudio, la flexibilidad que brindan las impresoras 3D pueden tener un uso dual y ser utilizadas para crear repuestos, herramientas o componentes a medida, como también para crear armas o un componente requerido para fabricar un dispositivo particular para causar daño, como por ejemplo un artefacto explosivo.

Entrando en las debilidades que presenta la tecnología en materia de ciberseguridad, podemos mencionar las siguientes:

- Muchos de estos equipos se valen de sistemas cerrados o embebidos para el control de los componentes que utiliza la impresora para su funcionamiento, los cuales constan de *software* (algunos de ellos de código abierto) que pueden tener vulnerabilidades que aún no cuentan con parches de seguridad o nuevas versiones de *firmware* para su solución; o situaciones más problemáticas, que son sistemas que no se pueden actualizar porque no serían compatibles con otros componentes. Para poder subsanar estas debilidades, es necesario seleccionar fabricantes de impresoras 3D que realicen el desarrollo integral de todo el *software* que controla su funcionamiento, o bien utilicen componentes estándares que ya cuenten con actualizaciones de seguridad periódicas. Esta debilidad también podría subsanarse aislando a estos equipos de la red corporativa, situación que en corto plazo podría requerir revisión como ocurre actualmente con las redes de OT o le restaría funciones colaborativas al sistema.
- El segundo aspecto viene de la mano con la integración que pueden tener las impresoras con internet u otros sistemas, aun las impresoras 3D más básicas se pueden conectar a internet a través de otras aplicaciones denominadas middleware[6], de las cuales se podría perder el control y resultar en vulnerabilidades que pueden ser explotadas. Por lo tanto, más allá de las vulnerabilidades intrínsecas que pudiesen existir en la forma en que las impresoras se conecten a internet, al estar expuestas aumentan la superficie de ataque.
- Para la impresión de objetos, las impresoras 3D utilizan instrucciones exactas acerca de los movimientos que deben realizar para completar cada capa del modelo. Muchas de estas impresoras, especialmente las de código abierto, utilizan para brindar estas instrucciones un lenguaje llamado G-Code, el cual carece de mecanismos que garanticen la integridad del archivo de coordenadas, convirtiendo a estos en un set de instrucciones que pueden ser modificas maliciosamente antes que la impresora comience a trabajar y modificar el objeto que se desea crear (Nachreiner, 2018). Para solucionar esta vulnerabilidad se podría considerar que los creadores de los archivos G-Code los acompañen de un hash[7], de forma que pueda recalcularse esta función cuando se al momento de utilizarlos verificando su integridad de origen.

---

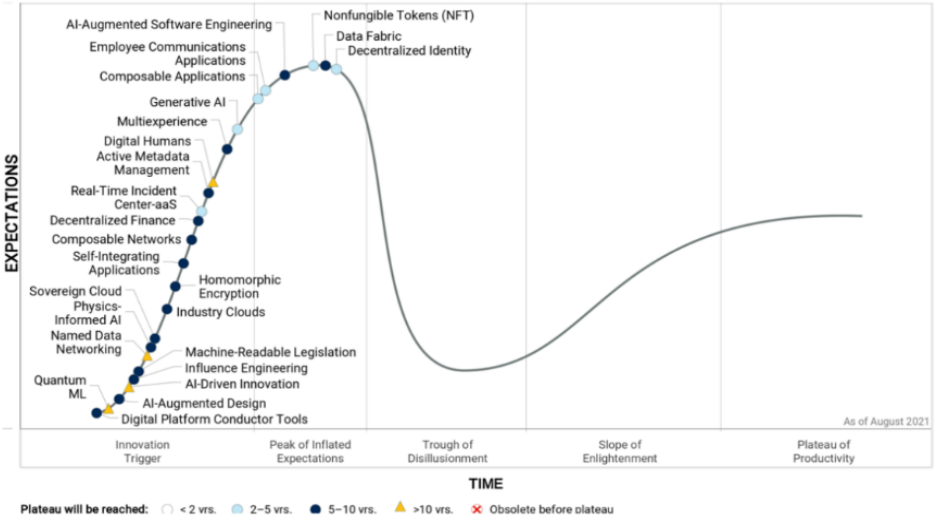
[6] Aplicaciones que se utilizan como medio de intercambio entre otras dos aplicaciones.

[7] Se denomina hash a un algoritmo que cumple con las características de no repetición (existe muy baja probabilidad de encontrar el mismo resultado para conjuntos de datos diferentes), y la unicidad, es decir el resultado de aplicar el algoritmo será siempre idéntico cada vez que se aplique al mismo conjunto de datos. Si algún cambio, por mínimo que sea, ocurre en los datos, cambiará entonces el resultado de la salida del algoritmo y por tanto el hash.

10. Computación cuántica

La computación cuántica tal vez es una de las tecnologías promisorias, aunque todavía no se sepa con claridad cuáles serán sus usos reales. Si bien hay muchos actores de importancia como universidades, grandes compañías y gobiernos trabajando activamente en su desarrollo, la realidad es que a pesar de ser una tecnología que tiene muchos avances, los usos sobre la misma se encuentran en el terreno de la investigación o dentro del dominio científico de la física. Es por este motivo que, a pesar de que lleva unos años desde haber salido a la luz, Gartner® nombra a esta tecnología como incipiente en la etapa de innovación de su clásico Hype Cycle[8] para tecnologías emergentes, augurando al menos 10 años para lograr ingresar en la etapa de productividad.

Gráfico 8
Madurez de las tecnologías emergentes



Fuente: "Gartner®, Hype Cycle for Emerging Technologies, 2021, Brian Burke, Melissa Davis, Philip Dawson, 11 August 2021".

Si bien en la actualidad existen computadoras cuánticas, las mismas son prototipos que están destinados a probar el resultado funcional de la tecnología. Se puede inferir que se trata de una tecnología que será de alcance restringido, lo cual supone que quien logre acceso a la misma supondrá una ventaja muy importante con el resto de sus competidores.

11. Tecnologías Biónicas

El concepto de "humanidad aumentada" se encuentra muy presente; no es inapropiado pensar que, en un futuro, la mayoría de las personas (o al menos una gran parte) tenga implantadas prótesis biónicas para aumentar el rendimiento de las funciones motrices, o chips implantados que permitan monitorear en tiempo real que es lo que está pasando con su cuerpo, o que ayuden a aumentar la capacidad intelectual. Estas funciones que hace algún tiempo parecían extraídas de la ciencia ficción, se están materializando con aplicaciones reales. Durante el año 2020 Elon Musk, fundador de Tesla y SpaceX entre otras empresas, anunció un producto llamado Neuralink[9] que consiste en la

[8] El Hype Cycle de Tecnologías Emergentes de Gartner®, es una representación gráfica de la madurez, adopción y aplicación comercial de tecnologías específicas.

[9] https://neuralink.com/.

implantación de chips capaces de medir la actividad cerebral en tiempo real y en un futuro podrían utilizarse para prevenir enfermedades neurológicas. Los beneficios y aplicaciones de las tecnologías biónicas parecieran estar orientados a la mejora del rendimiento de los seres humanos o a prolongar su vida, ya sea aumentando su rendimiento físico, por ejemplo, con prótesis biónicas que ayuden a un trabajador a mover un objeto pesado sin esfuerzo o daño a su salud, a prevenir enfermedades o a conocer en tiempo real y en todo momento el estado del cuerpo.

En 2019, en el Mobile World Congress (MWC) que se desarrolla en Barcelona todos los años, expertos de la firma Kaspersky presentaron un estudio advirtiendo que las prótesis biónicas podrían ser hackeadas y alertando acerca de las implicancias que esta tecnología podría tener (Kaspersky Lab, 2019). Pero el mayor desafío de seguridad en el campo de las tecnologías biónicas está en los derechos fundamentales y de la privacidad de las personas. La propiedad sobre los datos que se generan y se comparten a través de esta tecnología, el uso que se les dará y el acceso a ellos, el ciclo de vida y la prestación de servicios asociados, el pedido de remisión de esos datos de parte del propietario, son debates pendientes que parecieran ser necesarios antes de que ocurra la masificación de la tecnología, que las distintas organizaciones públicas y privadas deberían tener para que se establezcan pautas regulatorias para garantizar los derechos de las personas (Aguiar, 2021).

III. Gestión global de la ciberseguridad

Este apartado tiene como objetivo, presentar un resumen sobre la gobernanza en ciberseguridad en el mundo, explicando brevemente la situación jurídica, presentando los organismos de control y otras instituciones o iniciativas, y las acciones que dichas instituciones llevan adelante para mantener el orden, no solo en las infraestructuras críticas que afectan directamente a la logística, sino también en toda la sociedad, siendo actores claves en un escenario de creciente adopción de las tecnologías integrantes de la logística inteligente.

A. Organismos e iniciativas Internacionales

Tal como lo expresa Antonio Segura Serrano (2017), desde el Derecho internacional no se han adoptado iniciativas de normativas concretas dirigidas a afrontar cada una de las amenazas del ámbito del ciberespacio, salvo el caso de la Convención de Budapest de 2001. La doctrina y la práctica estatal han optado por una aplicación extensiva o análogas de las normas convencionales o consuetudinarias en vigor, consideradas por muchos como suficientes para hacer frente a estos desafíos. Que un solo Estado no pueda someter globalmente a su jurisdicción la actividad que tiene lugar en el ciberespacio, de naturaleza transfronteriza en buena parte, no implica que no se esté ejerciendo jurisdicción estatal en el mismo a través de las tradicionales bases de competencia territorial y personal, e incluso de forma indirecta, lo que permite territorializar el ciberespacio. Los Estados pueden ejercer su jurisdicción, y de hecho lo están haciendo, sobre la actividad cibernética que está orientada hacia un territorio determinado y tiene un efecto local, obviando que el instrumento utilizado, Internet, tiene trascendencia global, acción que podría facilitarse en el futuro si existe consenso internacional (Segura Serrano, 2017). Dicho consenso, como se verá a continuación, se ha estado produciendo en torno a algunas organizaciones internacionales como la Organización de Naciones Unidas, la Unión Europea (UE) o la Organización del Tratado del Atlántico Norte (OTAN), entre otras, delegando el poder de acción o control, a organizaciones internacionales existentes como Interpol y las agencias regionales asociadas, y otras organizaciones militares, a través de unidades especiales creadas para tal fin.

1. Programa Mundial Sobre Ciberdelincuencia - Oficina de las Naciones Unidas Contra la droga y el Delito (UNODC)

La UNODC promueve la creación de capacidad a largo plazo y sostenible en la lucha contra el delito cibernético mediante el apoyo a las estructuras y a las acciones nacionales. Específicamente, la UNODC se basa en su experiencia especializada en la respuesta de los sistemas de justicia penal para brindar asistencia técnica en el desarrollo de capacidades, la prevención y la concienciación, la cooperación internacional y la recopilación de datos, la investigación y el análisis sobre el delito cibernético; desarrollado por un comité intergubernamental, creado específicamente al efecto, compuesto por expertos representando a todas las regiones, para realizar un estudio amplio del problema del delito cibernético y las respuestas al mismo por parte de los Estados Miembros, la comunidad internacional y el sector privado. Este trabajo incluye el intercambio de información sobre legislación nacional, mejores prácticas, asistencia técnica y cooperación internacional, para elaborar una convención internacional integral sobre la lucha contra el uso de tecnologías de la información y las comunicaciones con fines delictivos, establecido por la Asamblea General de las Naciones Unidas (United Nations, 2021).

a) Mandato

Según la resolución 65/230 de la Asamblea General y las resoluciones 22/7 y 22/8 de la Comisión de Prevención del Delito y Justicia Penal, el Programa Mundial sobre Delitos Cibernéticos tiene el mandato de ayudar a los Estados Miembros en su lucha contra los delitos cibernéticos mediante la creación de capacidad y la asistencia técnica.

b) Objetivos y alcance geográfico

El Programa Global está diseñado para responder de manera flexible, apoyando a los Estados Miembros para prevenir y combatir el ciberdelito de manera integral. El principal nexo geográfico para el Programa de Delitos Cibernéticos en 2017 son América Central, África Oriental, MENA y el Sudeste de Asia y el Pacífico, con objetivos clave de:

- **mayor eficiencia y eficacia en la investigación**, el enjuiciamiento y la adjudicación de delitos cibernéticos, especialmente la explotación y el abuso sexual infantil en línea, dentro de un marco sólido de derechos humanos; declarados específicamente por Naciones Unidas dentro de los Objetivos de Desarrollo Sostenibles.
- **respuesta a largo plazo eficiente y eficaz** de todo el gobierno al ciberdelito, incluida la coordinación nacional, la recopilación de datos y marcos legales efectivos, que conduzcan a una respuesta sostenible y una mayor disuasión.
- **fortalecimiento de la comunicación nacional e internacional** entre el gobierno, las fuerzas del orden y el sector privado con un mayor conocimiento público de los riesgos del ciberdelito.

c) Repositório de delitos informáticos

En 2015, la UNODC, en el marco de la Comisión de Prevención del Delito y Justicia Penal (CCPCJ), lanzó el repositorio de delitos cibernéticos, una base de datos central de legislación, jurisprudencia y lecciones aprendidas sobre delitos cibernéticos y pruebas electrónicas. El repositorio de delitos informáticos tiene como objetivo ayudar a los países en sus esfuerzos por prevenir y enjuiciar eficazmente a los delincuentes cibernéticos.

El repositorio consta de tres partes que tienen como objetivo facilitar los esfuerzos de los Estados contra el delito cibernético:

i) La Base de datos de legislación, que contiene legislación sustantiva y procesal sobre delitos cibernéticos y pruebas electrónicas de más de 180 países y se puede buscar por país, tipo de delito cibernético y aspectos procesales. La base de datos contiene extractos de leyes pertinentes a los delitos cibernéticos y cuestiones transversales y permite a los usuarios acceder a documentos legislativos completos;

ii) La Base de datos de jurisprudencia, que contiene jurisprudencia y registros de operaciones exitosas de aplicación de la ley, sobre delitos cibernéticos y delitos relacionados con pruebas electrónicas. Esto permite a los usuarios ver cómo los Estados abordan los casos de delitos cibernéticos tanto operativamente como en sus tribunales;

iii) La base de datos de lecciones aprendidas, que contiene prácticas y estrategias nacionales para prevenir y combatir el delito cibernético. La información recopilada en esta base de datos se ha recopilado en el marco del Estudio integral de la UNODC sobre el delito cibernético y se complementa con estrategias nacionales de ciberdelincuencia y ciberseguridad.

2. Consejo de Europa - Convenio de Budapest

El Convenio sobre la Ciberdelincuencia, conocido como Convenio de Budapest, fue elaborado durante el 2001 por el Consejo de Europa, con la activa participación de los Estados involucrados, con el fin de combatir los delitos informáticos. El mismo, al ser ratificado por más de sesenta países del resto del mundo le ha conferido carácter de internacional.

a) Definiciones y Lineamientos

De acuerdo con la definición oficial, el Convenio de Budapest (CETS No.185), sancionado el 23 de noviembre de 2001 por el Comité de ministros del Consejo de Europa, es:

> "El primer tratado internacional sobre delitos cometidos a través de Internet y otras redes informáticas, que se ocupa especialmente de las infracciones de los derechos de autor, el fraude informático, la pornografía infantil y las violaciones de la seguridad de la red. También contiene una serie de poderes y procedimientos, como la búsqueda de redes informáticas y la intercepción".

El mismo establece una política penal común y alineada entre países, orientada a la protección de la sociedad contra la ciberdelincuencia. Como es conocido, en la Unión Europea los estados miembros renuncian a parte de su soberanía a favor de la Unión, lo cual ha facilitado la legislación en materia de ciberseguridad en la región. El objetivo del convenio se alcanza tipificando los delitos informáticos para todas las naciones, unificando normas procesales y a través de una cooperación internacional armónica.

A la fecha de su sanción, se transformó en el único instrumento internacional vinculante y en una guía para que los países desarrollen legislaciones nacionales contra el Cibercrimen. El artículo 37 establece que los Estados no miembros del Consejo de Europa y que no hayan participado en la elaboración del tratado, pueden adherirse por invitación del Comité de ministros del COE. A la fecha ya son más de 60 países a nivel global los que se han adherido al tratado (Estévez, 2020).

B. Entes reguladores

1. Unión Internacional de Telecomunicaciones (UIT)

La UIT es el organismo especializado de las Naciones Unidas para las tecnologías de la información y la comunicación (TIC), a cargo de la reglamentación, normalización y desarrollo de las

telecomunicaciones en todo el mundo. En general, la normativa generada por la UIT está contenida en un amplio conjunto de documentos denominados «Recomendaciones», agrupados por «Series». Cada serie está compuesta por las recomendaciones correspondientes a un mismo tema, por ejemplo: Tarificación, Mantenimiento, etcétera. Si bien las recomendaciones emitidas no revisten el carácter de normativa internacional, su contenido es considerado como obligatorio por las administraciones y empresas operadoras a nivel de relaciones internacionales.

a) Funciones y Lineamientos

- Desarrolla estándares que facilitan la interconexión de las infraestructuras de comunicación nacionales con las redes globales, permitiendo un fluido intercambio de información desde cualquier país;
- Trabaja para integrar nuevas tecnologías en la red de telecomunicaciones global, para fomentar el desarrollo de nuevas aplicaciones tales como Internet, el correo electrónico y los servicios multimedia;
- Gestiona el reparto del espectro de frecuencias radioeléctricas y de las órbitas de los satélites, recursos naturales limitados utilizados por una amplia gama de equipos incluidos los teléfonos móviles, las radios y televisiones, los sistemas de comunicación por satélite, los sistemas de seguridad por navegación aérea y marítima, así como por los sistemas informáticos sin cable;
- Se esfuerza por mejorar la accesibilidad a las telecomunicaciones en el mundo en desarrollo a través del asesoramiento, la asistencia técnica, la dirección de proyectos, los programas de formación y recursos para la información, y fomentando las agrupaciones entre las empresas de telecomunicaciones, los organismos de financiación y las organizaciones privadas;
- Engloba a 193 países miembros y unas setecientas entidades del sector privado, que trabajan juntos para la evolución de los sistemas de telecomunicaciones.

En virtud de un Memorando de Entendimiento entre la UIT y la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), firmado con ocasión del Foro de la CMSI celebrado en mayo de 2011 en Ginebra, ambas organizaciones se comprometen a colaborar para ayudar a los Estados Miembros de la UIT y de las Naciones Unidas a mitigar los riesgos que plantea la ciberdelincuencia (International Telecomunications Union, United Nations, 2021).

2. Agencia de la Unión Europea para la Ciberseguridad – ENISA

La ENISA, Agencia de la Unión Europea para la Ciberseguridad, es un centro de conocimientos especializados para la seguridad cibernética en Europa. La ENISA ayuda a la UE y los países que la integran a estar mejor equipados y preparados para prevenir, detectar y dar respuesta a los problemas de seguridad de la información y ayudando a elaborar las políticas y la legislación de la UE sobre seguridad de las redes y de la información. Ofrece soluciones y asesoramiento prácticos a los sectores público y privado de los países de la UE y a las instituciones europeas. Esto incluye:

- Organizar ejercicios de gestión de crisis cibernéticas a escala europea
- Contribuir al desarrollo de estrategias nacionales de ciberseguridad
- Fomentar la cooperación entre los equipos de respuesta a emergencias informáticas y la creación de capacidades.

También publica informes y estudios sobre cuestiones de ciberseguridad. Ha elaborado estudios sobre:

- Seguridad de la nube
- Protección de datos
- Tecnologías potenciadoras de la privacidad y cómo garantizar la privacidad de las nuevas tecnologías
- Servicios de identificación y de confianza electrónicos
- Identificación de ciber amenaza

C. Organismos de control

1. Interpol

La Organización Internacional de Policía Criminal (Interpol), organización intergubernamental que cuenta con 194 países miembros, interactúa con la policía de estos países facilitando el intercambio y acceso a información sobre delitos y delincuentes, disponiendo también de apoyo técnico y operativo.

a) Estrategia Mundial Contra la Ciberdelincuencia

La estrategia comprende cinco líneas de acción, con el objetivo común de ayudar a los países miembros a identificar ataques cibernéticos y sus autores:

i) Evaluación y análisis de amenazas, seguimiento de las tendencias para detectar e identificar a los autores o grupos de acción.

ii) Acceso a los datos relacionados con ataques cibernéticos y explotación de estos y a las herramientas, para consolidar la recopilación y mejorar su explotación.

iii) Gestión de pruebas digitales orientada a la investigación y el uso jurídico de ellas, considerando la recopilación y conservación legal de pistas informáticas de forma que estas resulten inteligibles y aceptables para el sistema judicial.

iv) Correlación de información digital y física estableciendo puentes a fin de identificar la ubicación de los posibles autores.

v) Armonización e interoperabilidad en lo global, alentando la armonización legislativa.

b) Alcance y Aplicación

La estrategia aborda la "ciberdelincuencia pura", delitos contra ordenadores y sistemas de información en los que el objetivo es acceder sin autorización a un dispositivo o denegar el acceso a un usuario legítimo. Al mismo tiempo Interpol reconoce la importancia de la lucha contra como el fraude financiero y el uso terrorista de los medios sociales procesados en medios cibernéticos. El programa está dirigido desde el Complejo Mundial de Interpol para la Innovación en Singapur, donde se encuentra el centro Cyber Fusion, haciendo uso de las capacidades policiales de Interpol.

c) Líneas de Trabajo

- Respuesta a las ciberamenazas

  En colaboración con una serie de socios que se dedican a la ciberseguridad en el sector privado, se intercambian datos actualizados sobre amenazas, tendencias y riesgos, con los cuales se realiza ciberinteligencia, que sirve para desarrollar, en los países participantes, estrategias de prevención y desarticulación de los peligros existentes y anticipación a los emergentes.

- Operaciones contra la Ciberdelincuencia

  En colaboración con los países miembros, el sector privado y los equipos nacionales de respuesta a emergencias informáticas, se coordinan investigaciones y operaciones transnacionales sobre delincuencia en todo el planeta.

d) Grupos de trabajo

Estas iniciativas, son desplegadas en tres fases, buscando abordar a distintos niveles y variados enfoques la problemática de la ciberdelincuencia.

- Grupo Mundial de Interpol de expertos en ciberdelincuencia, el cual sirve de plataforma para el intercambio de información y buenas prácticas en materia cibernética, con miras a apoyar a los organismos encargados de la aplicación de la ley. También ayuda a INTERPOL a desarrollar estrategias para los asuntos y proyectos relacionados con la ciberdelincuencia.
- Grupos de trabajo regionales sobre ciberdelincuencia para jefes de unidad, comprendiendo las regiones de África, América, Asia, Europa y Cercano Oriente. Liderados por jefes de unidades que se reúnen periódicamente formulando propuestas de políticas y la ejecución de proyectos para combatir la ciberdelincuencia según las necesidades de cada región.
- Conferencia Interpol-Europol sobre la ciberdelincuencia, la cual se realiza anualmente y reúne a expertos en cibernética procedentes de organismos encargados de la aplicación de la ley, sector privado e instituciones académicas a fin de debatir en profundidad acerca de las amenazas cibernéticas más recientes y analizar cómo combatirlas mediante una respuesta colectiva global (Interpol, 2021).

2. Organizaciones militares

a) Organización del Tratado del Atlántico Norte (OTAN)

Una historia de resiliencia icónica

En el año 2007 el gobierno de Estonia decidió mudar el icónico Soldado de Bronce, que fuera instalado originalmente en 1947 por las autoridades de la Unión Soviética y llamado Monumento a los Libertadores de Tallin, a un cementerio militar de los suburbios de dicha ciudad; como es conocido, el monumento representa la controversia entre dos sociedades, por un lado aquellos de habla rusa lo consideran la victoria de la URSS sobre el ejército Alemán durante la segunda guerra mundial, mientras que para quienes son de etnia estonia, representa a un ejército que no lo consideran libertador, sino más bien todo lo opuesto. La decisión generó protestas en la sociedad de origen soviético y las mismas fueron enardecidas por publicaciones de noticias falsas en los medios digitales, que indicaban que con la mudanza del monumento se estaban destruyendo no solo la estatua, sino también las tumbas cercanas de soldados soviéticos. EL 27 de abril de ese año, Tallin estalló como consecuencia de este hecho y hubo dos noches de disturbios que dejaron un saldo de un muerto, más de un centenar y medio de heridos y mil detenidos (McGuinness, 2007). En los días que continuaron, Estonia fue objetivo para la instalación de botnets[10] y recepción de un volumen muy elevado de correos electrónicos de tipo spam[11], llevando a un colapso muchos servicios digitales que, entre otras consecuencias, provocó la imposibilidad de comunicarse por correo electrónico a los empleados del

[10] Se llaman botnets a las redes formadas por computadoras que han sido víctimas de un *software* capaz de utilizar los recursos de procesamiento y memoria de un sistema informático para trabajar de manera conjunta con el fin de procesar de manera distribuida y anónima, cadenas relacionadas, por lo general, con delitos informáticos como el envío masivo de correo basura, distribución de información de pornografía infantil y ataques a sistemas que dejan de responder por la gran cantidad de peticiones simultáneas recibidas.

[11] Correo electrónico no solicitado que se envía a un gran número de destinatarios con fines publicitarios o comerciales.

estado, los medios de comunicación no podían publicar noticias actualizadas, y toda la población se vio imposibilitada de operar los cajeros automáticos y los servicios en línea de los bancos estonios. A partir de este incidente relacionado con la ciberguerra, Estonia ha implementado una Unidad de Ciberdefensa que congrega voluntariamente a grandes y costosos talentos del sector privado que se reúnen concientizados del valor que la ciberseguridad representa para su país; esta decisión estratégica ha convertido en Estonia en un referente de la ciberseguridad al punto de transformarse en el centro de operaciones de ciberinteligencia de la Organización del Tratado del Atlántico Norte.

Este evento configura los primeros antecedentes de ciberseguridad en la OTAN, ya que en el año 2008 Estonia propuso crear en su territorio el Centro de Excelencia cooperativa de ciberdefensa de la OTAN (CCD CoE) en Tallin; instalación de investigación y capacitación que se ocupa de la educación, la consulta, las lecciones aprendidas, la investigación y el desarrollo de la defensa cibernética. Aunque no forma parte de la Estructura de Mando de la OTAN, el CCD CoE ofrece conocimientos y experiencia de reconocido mundial a los Estados miembros.

En la Cumbre de Gales en septiembre de 2014, la OTAN confirmó que el derecho internacional es aplicable al ciberespacio y desde ese momento, ha desarrollado acciones en consecuencia; en la Cumbre de Varsovia de 2016 se reafirmó el mandato defensivo y se reconoció al ciberespacio como un ámbito de operaciones en el que la OTAN debe defenderse con la misma eficacia que lo hace en el aire, en tierra y en el mar, dado que **la mayoría de las crisis y conflictos actuales tienen una dimensión cibernética**. Previamente en febrero del mismo año la organización realizó un acuerdo técnico de cooperación sobre ciberdefensa con la Unión Europea (UE) con el objetivo de reforzar la cooperación en esta materia, especialmente en las áreas de intercambio de información, formación, investigación y ejercicios. A partir de ese momento, se ha mejorado el intercambio de información y la asistencia mutua para prevenir, mitigar y recuperarse de los ataques cibernéticos y se formaron equipos de reacción cibernética inmediata que están en espera para ayudar a los aliados, las 24 horas del día, si así lo solicitan y lo aprueban. Luego, en la Cumbre de Bruselas de 2018, los Aliados acordaron establecer un nuevo Centro de Operaciones del Ciberespacio en Mons, Bélgica, como parte de la Estructura de Mando fortalecida de la OTAN. También concertaron que la OTAN puede aprovechar las capacidades cibernéticas nacionales para sus misiones y operaciones.

En la Cumbre de la OTAN en junio de 2021, los Estados Miembros reafirmaron su compromiso de actuar de conformidad con el derecho internacional, incluida la Carta de las Naciones Unidas, el derecho internacional humanitario y el derecho internacional de los derechos humanos para promover un ciberespacio libre, abierto, pacífico y seguro; y proseguir los esfuerzos para mejorar la estabilidad y reducir el riesgo de conflicto.

La ciberdefensa se ha integrado en las iniciativas de Defensa Inteligente de la OTAN, la cual permite a los países trabajar juntos para desarrollar y mantener capacidades que no podrían hacerlo por sí solos, y liberar recursos para desarrollar otras capacidades. Los proyectos de Smart Defence en ciberdefensa incluyen actualmente la Plataforma de Intercambio de Información sobre *Malware* (MISP) y el proyecto *Smart Defence Multinational Cyber Defence Capability Development* (MN CD2) (NATO, 2021).

El Centro de Defensa Cibernética de Tallin es uno de los 21 Centros de Excelencia acreditados (COE) para la formación en aspectos técnicamente exigentes de las operaciones de la OTAN. Estos centros están estrechamente vinculados a la Transformación del Mando Aliado y promueven los objetivos de transformación establecidos por la Alianza.

3. Organizaciones privadas – Colaboración con organismos oficiales - Gestión pública-privada

Las empresas privadas, desde sus especializaciones: fabricantes, integradores, consultores u otras, ofrecen soluciones a la lucha contra la ciberdelincuencia, estableciendo vínculos de colaboración, que puedan ser con o sin fines de lucro, con los organismos oficiales; compartiendo ambas partes conocimientos especializados, tecnologías y recursos a fin de abordar los problemas a los que se enfrentan las fuerzas del orden y la sociedad en su conjunto. Las entidades oficiales, para la aceptación de esta colaboración, cuentan con procedimientos de transparencia y responsabilidad que se traducen en estrictas medidas de seguridad para garantizar que las contribuciones del sector privado (tecnológicas, financieras o de otra índole) se gestionen adecuadamente en el objetivo de contribuir en la búsqueda de lograr un mundo más seguro (Aguilar, 2017).

Los organismos oficiales encuentran en este proceder una importante ayuda para colmar brechas, mejorar su oferta de servicios o conocimientos técnicos a partir de la perspectiva dinámica de las nuevas tecnologías que las entidades privadas ofrecen. Esta cooperación suele adoptar la forma de financiación, aunque a menudo implica la puesta a disposición de personal, expedición de licencias de *software*, uso de equipos y edificios, y otras donaciones en especie.

D. Organismos e iniciativas regionales

El crimen en línea, tempranamente identificado como de características transnacionales en cuanto a ejecución y a sus perjuicios consecuentes, impulsó a los bloques regionales a reaccionar conforme a la escala que el fenómeno evidenciaba; el abordaje al mismo mediante una visualización de conjunto promoviendo la unificación de criterios legales y operativos, cooperación participativa sobre la información obtenida tanto desde la experiencia como de la investigación, asesoramiento técnico mutuo tanto desde bases tecnológicas como presencial; y todas aquellas medidas que surjan necesarias en la evolución del fenómeno delictivo.

1. Promovedores de políticas y lineamientos

Como se describió previamente en la sección Internacional, puede señalarse al Convenio de Budapest sobre delitos cibernéticos, impulsado por la Unión Europea, cuyo proceso de desarrollo inicial data del año 2001, como el primer tratado internacional que busca hacer frente a los ciberdelitos. La Organización de los Estados Americanos a través de sus organismos, oportunamente impulsa el desarrollo de políticas y acciones en el mismo sentido y adicionalmente promueve que sus Estados miembros adhieran al Convenio de Budapest; buscando consolidar una base homogénea a nivel mundial en la lucha contra el ciberdelito.

a) OEA - Comité Interamericano Contra el Terrorismo (CICTE). Programa de Ciberseguridad

El Comité Interamericano contra el Terrorismo, ha implementado un programa de Ciberseguridad, beneficiando a todos los países integrantes de la OEA a excepción de Cuba, consolidándose como líder en la misma en la provisión de iniciativas de investigación, fortalecimiento de la capacidad técnica y desarrollo de políticas de ciberseguridad en el continente. El programa se centra en tres pilares:

i) Desarrollo de políticas, el programa ayuda a los Estados miembros de la OEA a desarrollar estrategias nacionales o regionales de ciberseguridad que involucren a todas las partes interesadas relevantes y que se ajusten a la situación legislativa, cultural, económica y estructural de cada país y apoyen las evaluaciones a nivel nacional sobre la capacidad y la madurez de la ciberseguridad.

ii) Creación de capacidad: mediante el establecimiento y desarrollo de los equipos nacionales de respuesta a incidentes de seguridad informática (CSIRT) existentes, brindando asistencia técnica y oportunidades de ejercicio para fortalecer las instituciones y organizaciones nacionales y regionales. También se trabaja en las estrategias para el desarrollo de profesionales en la materia.

iii) Investigación y divulgación: El programa desarrolla documentos técnicos, conjuntos de herramientas e informes basados en investigaciones para guiar a los responsables de políticas, CSIRT, operadores de infraestructura, organizaciones privadas y la sociedad civil, destacando los desarrollos actuales e identificando los problemas y desafíos clave de seguridad cibernética en la región.

Los objetivos del programa de ciberseguridad son:

- Apoyar a los Estados Miembros de la OEA en el desarrollo de capacidades técnicas y políticas para prevenir, identificar, responder y recuperarse exitosamente de incidentes cibernéticos.
- Mejorar el intercambio de información, la cooperación y la coordinación sólidas, efectivas y oportunas entre las partes interesadas en seguridad cibernética a nivel nacional, regional e internacional.
- Aumentar el acceso al conocimiento e información sobre amenazas y riesgos cibernéticos por parte de los interesados públicos, privados y de la sociedad civil, así como los usuarios de Internet.

2. Entes reguladores

En América, la constitución de entes reguladores a nivel de bloque se encuentra en proceso de desarrollo a través de distintas iniciativas regionales, partiendo entre otros, del impulso dado por la Organización de los Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID), promoviendo, a partir del Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM, por sus siglas en inglés), el desarrollo o mejora de estrategias nacionales de ciberseguridad. Asimismo, es también de destacar la preocupación sobre la temática, manifestada por los países de la Alianza del Pacífico y del Mercosur, expresada En el Plan de Acción de Puerto Vallarta.

a) CSIRT Américas

En 2016 se realizó el lanzamiento de CSIRT Américas, una plataforma que permite la cooperación regional y el intercambio de información entre los equipos de respuesta a incidentes gubernamentales y nacionales de los Estados Miembros de la OEA. Sobre el modelo de Madurez de la Capacidad de Ciberseguridad, el que define cinco dimensiones para el abordaje a la ciberseguridad:

i) política y estrategia,

ii) cultura y sociedad,

iii) educación, capacitación y habilidades,

iv) marcos legales y regulatorios, y

v) estándares, organizaciones y tecnologías (BID y OEA, 2020).

b) Plan de acción de Puerto Vallarta entre los países de la Alianza del Pacífico y del Mercosur – Agenda digital

El objetivo primario de esta iniciativa puede sintetizarse en las palabras del entonces presidente pro tempore de la Alianza del Pacífico, Enrique P. Nieto:

"El plan de acción de Puerto Vallarta establece medidas concretas para facilitar el comercio de bienes, impulsar la internacionalización de pequeñas y medianas empresas y fomentar la economía de conocimiento".

El apartado Agenda Digital del plan de acción, cita como uno de los lineamientos de la iniciativa, "Intercambiar experiencias en materia de políticas nacionales sobre ciberseguridad, protección de datos personales y evaluar la posibilidad de trabajar en lineamientos comunes", lo cual sienta la base de trabajo sobre el desarrollado en común de ambas alianzas (Mercosur, 2018).

Actualmente promover la confianza en línea, la privacidad, la protección de datos y la ciberseguridad, se encuentra dentro de la Hoja de ruta para el mercado digital de la Alianza del año 2021 (Alianza del Pacífico, 2021), y en el acta de la 2da reunión de 2021 del Mercosur, los representantes se comprometieron a revisar el "Cuestionario MERCOSUR sobre Ciberseguridad" presentado por la Delegación de Argentina y las delegaciones coincidieron en realizar consultas con los diferentes órganos del MERCOSUR, con el fin de identificar aquellos temas de mayor prioridad para orientar los esfuerzos hacia el desarrollo de servicios transfronterizos de gobierno digital (Mercosur, 2021).

3. Organizaciones policiales

a) Ameripol

La Comunidad de Policías de América (AMERIPOL), es un mecanismo de cooperación integrado por 33 cuerpos policiales nacionales y 26 organismos observadores, cuyo propósito es promover y fortalecer la cooperación policial en materia técnico-científica, de capacitación, así como para dinamizar y hacer más efectivo el intercambio de información con fines de inteligencia (Ameripol, 2021). Se conducen acciones sostenidas de investigación criminal y asistencia judicial entre los cuerpos de policía e instituciones homólogas de América. En cuanto a la ciberseguridad trabaja coordinando acciones de a nivel regional con las policías nacionales y con Interpol a nivel internacional.

4. Convenios

a) EL PAcCTO - Europa Latinoamérica Programa de Asistencia contra el Crimen Transnacional Organizado

Programa de cooperación internacional financiado por la Unión Europea que busca contribuir a la seguridad y la justicia en América Latina a través del apoyo a la lucha contra el crimen transnacional organizado. Los países americanos participantes son: Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Honduras, México, Nicaragua, Panamá, Paraguay, Perú y Uruguay (EL PAcCTO, 2021).

El programa está coordinado por:

- La Fundación Internacional y para Iberoamérica de Administración y Políticas Públicas (FIIAPP), que es una fundación del sector público estatal (F.S.P.). Trabaja al servicio de las administraciones públicas, gestionando la participación de sus diferentes órganos en programas y proyectos de cooperación técnica, impulsando de esta forma su internacionalización.
- Expertise France, Agencia Francesa de Cooperación Técnica Internacional. Su misión es satisfacer la demanda de los países socios que quieran mejorar la calidad de sus políticas públicas para responder a los desafíos ambientales, sociales, económicos o de seguridad a los que se enfrentan.

Las estrategias desarrolladas por el programa se basan sobre los pilares de cooperación policial, sistemas de justicia y penitenciarios, atendiendo ejes transversales entre los que se encuentra el de cibercrimen, vinculado con el programa Support de Ameripol e Interpol.

IV. El contexto en América Latina y el Caribe

A. Gobernanza de la ciberseguridad en ámbito público y privado

Internet está compuesta por redes operadas independientemente por diferentes actores que mantienen una variedad de modelos comerciales. Históricamente, el sistema ha evolucionado de manera colaborativa y global, y es razonable suponer que esta narrativa continuará caracterizándolo, con independencia de la aparición de los distintos participantes que, en el tiempo, se han sumado al fenómeno global. Inicialmente la red se desarrolla en el ámbito privado, sin mayor intervención de los Estados, produciéndose la primera intervención regulativa de tipo "restriccionista", durante los años 2000-2005, ante la explosión de volumen que registra la Internet en la última década del siglo XX y complementariamente considerar que en el ciberespacio existen actividades y expresiones que deben ser reguladas y administradas, incluyendo también la posibilidad de ser bloqueadas. Entre las actividades indeseadas, se registra cada vez con mayor impacto la ciberdelincuencia, esta irrupción impone una revisión del concepto de gobernanza para la Internet en la se acepta resignar parte del amplio concepto de libertad, impronta característica desde sus inicios, buscando encontrar equilibrio con las acciones de seguridad, que los ciberataques de los últimos años, explican y justifican plenamente.

En el año 2004, los Estados miembros de la Organización de Estados Americanos aprobaron un marco regional coordinado llamado: "Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética", generando una instancia pionera en cuanto a cooperación internacional que promueve el desarrollo de una cultura cibernética que genere medidas eficaces en la lucha contra la delincuencia cibernética, involucrando en las mismas tanto a los gobiernos como a los actores de la industria y entidades normalizadoras públicas y privadas. Comprendiendo que uno de los principales retos de la gobernanza de Internet en Latinoamérica es la ciberseguridad (Iniseg, 2021).

El despliegue y alcance desarrollado por el ciberdelito, en la segunda década del presente siglo, coloca a la ciberseguridad en un papel protagonista dentro del escenario internacional, encontrando a la región con una serie de fortalezas, de las que podrían citarse el alto porcentaje de conexión a la

Internet, el desarrollo de marcos normativos nacionales y regionales ad-hoc, y la adhesión a convenios internacionales, como por ejemplo el Convenio de Budapest sobre el Delito Cibernético (OEA, 2008).

No obstante, debe también exponerse ciertas debilidades, que en distintas magnitudes se encuentran en todo el globo, acentuadas en América Latina y el Caribe:

- Infraestructura tecnológica atrasada o desactualizada.
- La masificación de los dispositivos móviles y por lo tanto de Android, sistema operativo muy frágil y expuesto al *malware*.
- La falta de profesionales y técnicos con sólida formación en el campo de la ciberseguridad que puedan prestar su asesoría a instituciones y empresas.

Ante estas consideraciones, tal vez sea acertado reformular la definición de gobernanza de Internet, comprendiendo el rol central que ha adquirido la ciberseguridad y concluyendo que su gobernanza es el factor determinante en el presente y para el desarrollo futuro de la plataforma.

1. Situación en el ámbito privado, empresas internacionales y Pymes

El fenómeno de la ciberdelincuencia cuenta entre otras características, con la capacidad de afectar todo tipo de infraestructuras, con independencia de: sus funciones, competencias y volumen tecnológico, características de negocio, aplicación de uso y toda otra particularidad.

En el ámbito privado, centrando la visión en el medio empresario, el grado de maduración en cuanto a ciberseguridad está dado tanto por el nivel cultural adquirido como por la capacidad económica para implantar y sostener la infraestructura requerida en cada caso.

Pudiendo entonces analizarse por separado dos grandes espacios: el empresario de gran escala (considerando en este caso el internacional) y las pequeñas y medianas empresas.

a) Empresas Internacionales

En un reciente reporte Cyber Risk Index (CRI) de Trend Micro donde se calcula el índice de riego de las organizaciones, la compañía internacional de ciberseguridad dio a conocer que la región Latinoamericana se encuentra en riesgo moderado de ser víctima de ataques cibernéticos, arrojando un valor CRI positivo de 0.06, mientras que, en América del Norte, el mismo indicador resulta negativo con -1.27 de puntuación. El índice se calcula considerando la diferencia entre postura frente a la ciberseguridad de la organización y la probabilidad de ser atacada, considerando el riesgo máximo con un índice de -10 y el mínimo de 10 (TrendMicro Inc., 2021).

Mientras que el nivel global de riesgo es elevado, Latinoamérica destaca con una calificación de nivel moderado para la misma medición. Sobresaliendo también por ser la única región en especificar los dispositivos móviles como parte de la infraestructura que se teme pueda estar en riesgo de ataques, lo cual indicaría también la necesidad de adaptar medidas acordes a las tendencias laborales de la región a diferencia de otros territorios en el mundo.

En contraposición a estos datos alentadores los riesgos fundamentales para las empresas latinoamericanas se presentarían en la forma de desafíos con autoridad de nivel ejecutivo y prioridad de seguridad. Es decir, los sistemas en relación con los cargos más altos de las entidades requerirían mayores esfuerzos sobre la seguridad digital, en comparación con el resto.

b) Pequeñas y Medianas Empresas

Durante los primeros ocho meses del año 2021, en la región de Latinoamérica hubo 728 millones de intentos de infección, según los recolectores en línea de la firma de servicios de seguridad Kaspersky, lo cual significa un resultado en el orden de 35 ciberataques por segundo, representado un

incremento de 24% en relación con el mismo periodo del año anterior (Diazgranados, 2021). Al mismo tiempo, puede estimarse que el 40 % de los ataques que resultan efectivos y causar un daño mayor, afectan a organizaciones PyMES, produciendo un daño tal que, en muchos casos, estas no logran recuperarse. En Latinoamérica no existe una difusión de la infraestructura y esfuerzos que diferentes organismos realizan para luchar contra el ciberdelito, como se ha expuesto a lo largo del documento, lo cual resulta en desconocimiento por parte de las PyMES sobre el curso a seguir en caso de recibir un ciberataque. Además, paradigmáticamente se considera la publicación de estos eventos por parte de los afectados, como una debilidad comercial en lugar de una realidad intrínseca de la tecnología. En un reciente estudio de relevamiento de ataques perpetrados a organizaciones de América Latina y el Caribe, se detectó que aproximadamente de cada treinta casos denunciados por grandes compañías, solo una mediana empresa lo hizo. Resulta importante entonces, dada la gran cantidad de este tipo de organizaciones que en América Latina componen el ecosistema de la logística, y que, como se ha desarrollado, la resiliencia de la cadena es dependiente de todos sus integrantes, trabajar desde las organizaciones públicas en la concientización sobre la seguridad cibernética y exponer claramente los canales disponibles para denuncias y tratamiento de ellos.

c) Gobiernos y organizaciones gubernamentales

El Programa de Seguridad Cibernética del Comité Interamericano contra el Terrorismo de la Organización de Estados Americanos impulsado a través del Comité Interamericano contra el Terrorismo; promueve como objetivo proveer "iniciativas de investigación, fortalecimiento de la capacidad técnica y desarrollo de políticas de ciberseguridad en las Américas. El programa se centra en 3 pilares: desarrollo de políticas, desarrollo de capacidades (incluyendo capacitación y ejercicios cibernéticos), e investigación y divulgación"

Esta iniciativa pone en manos de los Estados miembros la implantación y desarrollo de los Equipos CSIRT con el mandato de desarrollar capacidad de gestión y registro, sobre los eventos de agresión acaecidos en cada país en un marco colaborativo regional. Por lo que cada gobierno toma, oportunamente, el rol ejecutivo preciso para el cumplimiento de este cometido.

Asimismo debe señalarse que la adhesión (a instancias de la Organización de Estados Americanos) y posterior ratificación al Convenio de Budapest sobre el Delito Cibernético, por parte de: Argentina, Chile, Colombia, Costa Rica, Panamá, Paraguay, Perú y República Dominicana; amplía el horizonte de colaboración a perspectiva internacional, con el reconocimiento de la normativa de la Unión Europea y la observación implícita de otras normas mundiales a partir de la interrelación de la UE con otras regiones del mundo.

El estudio "Ciberseguridad: riesgos, progreso y el camino a seguir en América Latina y el Caribe" emitido por la Organización de Estados Americanos en conjunto con el Banco Interamericano de Desarrollo (BID y OEA, 2020), informa que en comparación a la edición del año 2016 más de la mitad de los países de la región han mejorado su disposición hacia la ciberseguridad al desarrollar e implementar estrategias nacionales y/o marcos legales que permiten una mejor respuesta a las ciberamenazas, incluyendo mayor protección de los datos personales de los ciudadanos. No obstante, se observa la necesidad de aumentar los esfuerzos para robustecer la ciberseguridad; los avances en la región se encuentran limitados, en parte, por la ausencia de talento humano calificado (se estima un déficit de 600.000 personas destinadas a la seguridad en la región). La oferta académica se ha incrementado en carreras de pregrado y de grado en Colombia y Argentina, por ejemplo, pero el desafío sigue vigente debido a la creciente demanda.

Según el mismo informe, informe tres cuartas partes de los países carecen de planes de protección para sus infraestructuras críticas, manifestándose también la necesidad de desarrollar mayores capacidades sistemáticas y eficientes en cuanto a monitoreo y capacidad de respuesta ante

los incidentes; señalando finalmente la carencia de instancias centralizadoras de coordinación de las actividades de ciberseguridad.

Estas observaciones sobre los Estados miembros recaen finalmente sobre los Gobiernos nacionales y sus organismos dependientes, señalando una demanda de inversión en la materia, sobre la base de los informes BID-OEA, que revelan una pérdida anual en la región que ronda los $90.000 millones dólares, según estimaciones realizadas por el Registro de Direcciones de Internet de América Latina y Caribe (LACNIC por su sigla en Inglés), producto de los hechos delictivos por sí mismos sumados al impacto social y el económico sobre terceras partes indirectamente involucradas (OEA, 2016). El fenómeno se debe al nuevo concepto de hacker, que ha dejado de evolucionar en la tipología de este, en beneficio de la escala; es decir aumentando progresivamente los ataques.

En particular, el informe "Ciberseguridad: riesgos, progreso y ..." señala la conveniencia de tomar medidas para generar confianza entre los usuarios de servicios de comercio electrónico, debido a la importancia fundamental que la ciberseguridad tiene en esta actividad. La agregación de los países de la región al comercio electrónico determinó retos que se debieron afrontar, como el de la seguridad informática, ascendiendo al 45% de los comercios de la región como víctimas de este, llegando a afectar a más de 800.000 usuarios (Perdigón Llanes & Pérez Pino, 2020). La inversión que América Latina habría realizado en fortificar la seguridad lograría una reducción para 2018 de una tercera parte (Rivera Guerrero, Hablich Sánchez, & Berni Morán, 2018), no obstante, el informe BID-OEA 2020 recomienda aplicar mayores esfuerzos de mejoras sobre este particular.

Las iniciativas desarrolladas en la región, en el periodo de tiempo observado por dicho informe, revelan que algunos países, como por ejemplo Colombia y Argentina, han establecido normativas y políticas públicas sobre el comportamiento en el ciberespacio. Podría destacarse en el informe a Uruguay, como el país más avanzado de la región en establecer e invertir en estrategias de ciberseguridad.

V. Conclusiones y recomendaciones para la región

Durante el informe se ha logrado describir la ciberseguridad como un fenómeno intrínseco de las tecnologías de la información y particularmente de las participantes de la 4ta revolución industrial, del cual se cuenta con normativas internacionales (ISO/IEC 27000) capaces de dar tratamiento a la problemática de manera independiente al tamaño y complejidad de las organizaciones y procesos, para aumentar la resiliencia de estos. Al mismo tiempo se evidenciaron los modelos de Cyber Kill Chain y ATT&CK para entender y tratar el ciclo de vida de los ciberataques con la finalidad de neutralizarlos en las etapas tempranas y de esta manera evitar o minimizar el daño o perjuicio producido.

Se ha desarrollado y sustentado la manera de entender a la ciberseguridad como un sistema inmune resultando en los llamados sistemas de ciberinmunidad, concepto que resulta compatible con los modelos analizados y oportuno para dar el marco general de abordaje a una problemática que, al igual que en los casos biológicos, evidencian una superficie muy extendida para quien se defiende y una estrategia muy específica para quien ataca. El uso de la Inteligencia Artificial constituye una pieza central en la manera de analizar los eventos de la red de TI y OT detectando de manera prematura los incidentes cibernéticos.

Se abordó luego las estadísticas de incidentes ocurridos a nivel global y regional, determinando que el beneficio lucrativo y las limitaciones que aún existen para combatir el cibercrimen se ven evidenciados en el crecimiento incesante de los ataques en cantidad y costo promedio, atendiendo también a las variaciones y perfeccionamiento que se suceden a medida que se mejoran las barreras de defensa. Una variable que cobra dimensión a medida que se demanda más información de las redes operativas, es la afectación de servicios de infraestructura crítica, donde se pudo determinar que los efectos provocados por fallas de seguridad podrían no solo afectar la economía en general, sino también la estabilidad de la sociedad, considerando que, en determinados escenarios, un incidente cibernético podría derivar en un conflicto bélico.

La investigación determinó que el 60% de las causas de los incidentes queda en manos de las personas por desconocimiento o falta de preparación en materia de seguridad para gestionar su cotidianeidad.

A lo largo del análisis de resiliencia, se ha podido determinar la falta de preparación de la mayoría de las organizaciones para atender los ataques, evidenciada principalmente por la falta de visibilidad e interpretación técnica oportuna de los eventos que ocurren tanto en la red tradicional de TI como en las redes Operativas. Sin embargo, se ha podido establecer que no existe una relación directa entre la innovación y los ataques recibidos por una organización, ya que, según los datos analizados, han resultado en costos más elevados los ataques sufridos por las organizaciones que no comenzaron su proceso de transformación digital frente a las que sí lo han hecho, debiendo aclararse que en dicho proceso de transformación, los ataques vuelven a incrementarse en costos conforme crece la complejidad tecnológica y, en consecuencia, la dificultad para monitorear la actividad no deseada. Este análisis resulta también oportuno para entender que **no actualizarse hacia las nuevas tecnologías solo agrava la situación en términos de seguridad**.

Del análisis se interpreta que las contramedidas más efectivas están relacionadas con la preparación y concientización de los recursos humanos, y la ciberseguridad preventiva, utilizando técnicas de las etapas prematuras de los modelos CKC7 y ATT&CK (monitoreo permanente, mantener actualizados *software* y *hardware*, etc.), que han logrado reducir significativamente los tiempos de detección y costos totales de las brechas de seguridad.

Luego se abordó individualmente cada una de las tecnologías que participan del concepto de *Smart Logistics* encontrando que, en general, las tecnologías no cuentan con debilidades de seguridad por las cuales se deba desalentar su implementación. Por el contrario, desde el punto de vista de la ciberseguridad se encuentran problemáticas comunes que están relacionadas con sus procesos de implementación, como la privacidad de los datos y consecuentemente, el control de acceso a ellos. El resto de la atención debe dedicarse a la infraestructura de base y de comunicaciones y no escapa a la problemática preexistente.

Dentro de la observación se destacaría como potencialmente beneficiosas desde el punto de vista de la ciberseguridad las soluciones basadas en *blockchain*, principalmente para robustecer y extender los servicios de VUCE y PCS. Las soluciones basadas en inteligencia artificial son beneficiosas para tareas rutinarias o mecánicas, desde el punto de vista de la eficiencia operativa y también representan una oportunidad en la logística inteligente para la asistencia en la toma de decisiones mediante el análisis de grandes volúmenes de datos.

Según lo analizado, requieren especial atención las decisiones que se tomen sobre *IoT*, donde deberá seleccionarse cuidadosamente los componentes a utilizar de esta tecnología, teniendo en cuenta que una solución que impacta en una cadena de valor no puede realizarse con elementos diseñado para usos aislados o que carezcan de la información necesaria y ciclos de vida del producto claramente documentados. El uso de la futura Norma ISO/IEC 27400 proporcionaría un marco adecuado para evaluar la ciberseguridad.

En el análisis de las organizaciones gubernamentales internacionales, se podría concluir que tanto la Organización de Naciones Unidas, como la Organización de Estados Americanos y la Unión Europea, cuentan con una clara visibilidad de la problemática de la ciberseguridad, la cual evidencian en sus políticas, estrategias y agendas operativas. Lo mismo ocurre con Interpol, que está trabajando activamente a través de su red para actuar contra el cibercrimen. Una situación diferente y polarizada pareciera ser la de las organizaciones militares, pero que no sería pertinente al alcance del informe a excepción de las situaciones que podrían derivar de un evento relacionado con las infraestructuras críticas. En tal caso, no se ha detectado información que evidencie que las organizaciones militares latinoamericanas estén trabajando de manera orgánica sobre la dimensión cibernética de la seguridad nacional donde otros organismos la consideran inseparable.

De las evidencias analizadas se infiere que, a escala regional, el problema de la normativa sobre ciberseguridad no estaría en las organizaciones transnacionales sino más bien recaería en la

operatividad de cada estado respecto a los lineamientos acordados por sus representantes dentro de ellas, sobre todo en América Latina donde la soberanía jurídica se encuentra balcanizada, y pareciera necesitarse una agenda operativa para implementar los lineamientos transnacionales en el afán de alcanzar el bien común.

El informe identifica que la naturaleza de los problemas de ciberseguridad radica en el valor creciente de los datos, situación que seguirá en ascenso debido a que son ellos los protagonistas de la 4ta revolución industrial, por lo tanto, el déficit entre la demanda para atender estos problemas y la oferta de profesionales de seguridad seguirá en ascenso. Se ha encontrado un incremento en la oferta académica de grado y pregrado en algunos países de la región como síntoma inicial de los nuevos trabajos que demandará el futuro, pero se debe seguir trabajando en la ampliación curricular profesional en LAC. También sería conveniente incorporar contenidos apropiados a cada nivel de formación académica de manera de elevar la conciencia colectiva de ciberseguridad.

Considerar el asesoramiento profesional de seguridad desde la etapa de estudio de viabilidad y diseño de la transformación digital en logística, reduciría los riesgos del nuevo proceso productivo y los costos de una posible brecha de seguridad, por ejemplo, reduciendo la complejidad del ecosistema o diseñando estrategias que mejoren el gobierno de este.

Las organizaciones que aún no lo han hecho, deberían sin demoras construir su plan de continuidad de negocio, las que cuenten con él, revisarlo periódicamente. Se deberían realizar pruebas periódicas del mismo que incluyan el DRP, y con los resultados retroalimentar y mejorar el plan, en un ciclo de mejora continua. Cada prueba se debería realizar considerando que la contingencia real ocurre sin previo aviso.

Sostener el esfuerzo que los organismos internacionales vienen realizando desde el principio del siglo XXI en coordinar acciones y alinear políticas que gobiernen el entorno que se plantea a través de la inexistencia de fronteras para los datos como bienes patrimoniales e inmateriales, podría desencadenar en que el marco jurídico internacional se actualice contemplando este terreno, generando reglas claras y sanciones que favorezcan el marco de confianza y seguridad operativa, que demandan los modelos de negocio de la 4ta revolución industrial.

Bibliografía

Aguiar, A. R. (2021, 03 25). *Bussiness Insider*. Retrieved from La ciberseguridad como derecho humano: qué pasará con los datos que genera el cuerpo ante el auge de la 'humanidad aumentada' y los implantes conectados: https://www.businessinsider.es/humanidad-aumentada-tecnologia-cuales-son-desafios-831497.

Aguilar, L. J. (2017). *Ciberseguridad:la colaboración público-privada en la era de la cuarta revolución industrial (Industria 4.0 versus ciberseguridad 4.0)*. Salamanca: Universidad Pontificia de Salamanca. Retrieved from Ciberseguridad:la colaboración público-privada en la era de la cuarta revolución industrial (Industria 4.0 versus ciberseguridad 4.0): https://dialnet.unirioja.es/servlet/articulo?codigo=6156210.

Alianza del Pacífico. (2021). Retrieved from Hoja de ruta para el mercado digital de La Alianza: https://alianzapacifico.net/wp-content/uploads/2021/06/HOJA-DE-RUTA-PARA-EL-MERCADO-DIGITAL-REGIONAL-DE-LA-ALIANZA-DEL-PACIFICO.pdf.

Ameripol. (2021, 09 30). *Ameripol.org*. Retrieved from http://www.ameripol.org/portalAmeripol/ appmanager/ portal/desk? nfpb=true&_pageLabel=portals_portal_page_m3p2_content&content_id=20058.

Barleta, E., Pérez Salas, G., & Sánchez, R. (2019). *La revolución industrial 4.0 y el advenimiento de una logística 4.0 - Boletín FAL 375, número 7, 2019*. Santiago de Chile, Chile.

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

CEPAL. (2021). *Estado de la ciberseguridad en la logística de América Latina y el Caribe*. Santiago, Chile: Publicación de las Naciones Unidas. Retrieved from https://repositorio.cepal.org/bitstream/ handle/11362/47240/1/S2100485_es.pdf.

_____(2020). *La ciberseguridad en tiempos del COVID-19 y el tránsito hacia una ciberinmunidad*. Santiago de Chile, Chile: CEPAL.

Checkpoint LTD. (2020, 07 22). *Checkpoint Software Technologies LTD*. Retrieved from CYBER ATTACK TRENDS: 2020 MID-YEAR REPORT: https://research.checkpoint.com/2020/cyber-attack-trends-2020-mid-year-report/.

CISA. (2021, 02 26). *Cybersecurity and Infrastructure Security Agency*. Retrieved from NSA Releases Guidance on Zero Trust Security Model: https://us-cert.cisa.gov/ncas/current-activity/2021/02/ 26/nsa-releases-guidance-zero-trust-security-model.

Corporation, M. (2020, Marzo). *http://www.mitre.org.* Retrieved from MITRE ATT&CKÒ: Design and Philosophy: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf.

Coveware. (2021, 07 01). *Coveware*. Retrieved from Q2 Ransom Payment Amounts Decline as Ransomware becomes a National Security Priority: https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority.

Díaz, R. M., Valdéz Figueroa, L., & Pérez Salas, G. (2021, 07 01). Retrieved from Oportunidades y desafíos para la implementación de blockchain en el ámbito logístico de América Latina y el Caribe: https://www.cepal.org/es/publicaciones/47098-oportunidades-desafios-la-implementacion-blockchain-ambito-logistico-america.

Diazgranados, H. (2021, 08 31). *Kaspersky*. Retrieved from Ciberataques en América Latina crecen un 24% durante los primeros ocho meses de 2021: https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/.

EL PAcCTO. (2021, 09 20). *EL PacCto.eu*. Retrieved from https://www.elpaccto.eu/sobre-el-paccto/que-es-el-paccto/.

ENISA. (2016, 03 08). Retrieved from Big Data Security: https://www.enisa.europa.eu/publications/big-data-security.

ENISA. (2021, 02 11). *Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous Driving*. Retrieved from https://www.enisa.europa.eu/news/enisa-news/cybersecurity-challenges-in-the-uptake-of-artificial-intelligence-in-autonomous-driving.

Estévez, J. C. (2020, 01 06). *Telefónica*. Retrieved 06 15, 2021, from En qué consiste el convenio de Budapest y cómo regula la ciberdelincuencia: https://empresas.blogthinkbig.com/convenio-budapest-ciberdelincuencia/.

Fung, B. (2021, 06 10). *CNN en Español*. Retrieved from JBS dice que pagó US$ 11 millones de rescate tras ciberataque: https://cnnespanol.cnn.com/2021/06/10/jbs-dice-que-pago-us-11-millones-de-rescate-tras-ciberataque-trax/.

Gallagher, R., & Burkhardt, P. (2021, 07 29). *Bloomberg*. Retrieved from 'Death Kitty' Ransomware Linked to South African Port Attack: https://www.bloomberg.com/news/articles/2021-07-29/-death-kitty-ransomware-linked-to-attack-on-south-african-ports.

García, S. B. (2021, 07 22). *Ciber Prisma*. Retrieved from Ciberataque interrumpe operaciones portuarias en Sudáfrica: https://ciberprisma.org/2021/07/22/ciberataque-interrumpe-operaciones-portuarias-en-sudafrica/.

Ginter, A. (2013). Retrieved from Unidirectional Security Gateways: Stronger than firewalls: https://accelconf.web.cern.ch/ICALEPCS2013/papers/thcoba02.pdf.

Harán, J. M. (2019, 11 14). *We Live Security*. Retrieved from Ciberataque a Pemex afectó el 5% de las computadoras: https://www.welivesecurity.com/la-es/2019/11/12/ciberataque-pemex/.

Harán, J. M. (2021, 05 11). We Live Security. Retrieved from Ataque de ransomware a compañía de oleoducto afecta el suministro de combustible en Estados Unidos: https://www.welivesecurity.com/la-es/2021/05/11/ataque-ransomware-compania-oleoducto-colonia-pipeline-afecta-suministro-combustible-estados-unidos/.

IBM Inc. (2021, 07 01). *IBM*. Retrieved from How much does a data breach cost?: https://www.ibm.com/security/data-breach.

Iniseg. (2021, 06 18). Retrieved from Ciberseguridad en América Latina: análisis y perspectiva: https://www.iniseg.es/blog/ciberseguridad/ciberseguridad-en-america-latina-analisis-y-perspectiva/.

International Telecomunications Union, United Nations. (2021). *ITU*. Retrieved 06 18, 2021, from Sobre la Unión Internacional de Telecomunicaciones (UIT): https://www.itu.int/es/about/Pages/default.aspx.

Interpol. (2021). *Interpol*. Retrieved 07 10, 2021, from Asociaciones con los sectores público y privado: https://www.interpol.int/es/Delitos/Ciberdelincuencia/Asociaciones-con-los-sectores-publico-y-privado.

ISO/IEC. (2021, 10 01). Retrieved from ISO/IEC DIS 27400-Cybersecurity — *IoT* security and privacy – Guidelines: https://www.iso.org/obp/ui/#iso:std:iso-iec:27400:dis:ed-1:v1:en.

Isotopy. (2021, 03 30). Retrieved from Realidad Virtual / Aumentada, seguridad y ciberdelitos: https://isostopy.com/realidad-virtual-aumentada-seguridad-y-ciberdelitos/.

Jackson, K. (2020, 02 24). *Science Node*. Retrieved from The real price of deepfakes: https://sciencenode.org/feature/Fake%20news,%20real%20problems.php.

Kaspersky Lab. (2021, 10 01). Retrieved from ¿Es peligrosa la tecnología 5G? Pros y contras de la red 5G: https://www.kaspersky.es/resource-center/threats/5g-pros-and-cons.

_____(2019, 03 04). *Analizamos la seguridad de las prótesis biónicas*. Retrieved from https://www.kaspersky.es/blog/securing-prosthetic-arm/17936/.

Katabella, R. (2021, 09 25). *The Epoch Times*. Retrieved from Importante puerto de EE.UU. fue el objetivo de un ciberataque en agosto: Funcionarios de CISA: https://es.theepochtimes.com/importante-puerto-de-ee-uu-fue-el-objetivo-de-un-ciberataque-en-agosto-funcionarios-de-cisa_896407.html.

Leonhard, G. (2016). *Technology vs. Humanity*. Fast Future Publishing.

Lockheed Martin. (2021). Retrieved Agosto 08, 2021, from Proactively detect persistent threats: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

Marsh. (2019). *Marsh McLennan*. Retrieved Agosto 8, 2021, from Encuesta de Percepción del Riesgo Cibernético en Latinoamérica 2019: https://www.marsh.com/ar/es/insights/research/marsh-microsoft-encuesta-percepcion-riesgo-cibernetico-2019.html.

Mceleny, C. (2015, 06 23). Retrieved from Tim Berners-Lee: AI will not be running a robot with a body, it will run corporations: https://www.campaignlive.co.uk/article/tim-berners-lee-ai-will-not-running-robot-body-will-run-corporations/1352752?src_site=marketingmagazine.

McGuinness, D. (2007, Mayo 6). *BBC Noticias*. Retrieved from Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país: https://www.bbc.com/mundo/noticias-39800133.

Mercosur. (2021, 08 10). *Mercosur - Calendario*. Retrieved from Acta 2/2021: https://calendario.mercosur.int/public/reuniones/doc/8626.

_____(2018, 07 24). Retrieved from Cartilla de la Cuidadanía del Mercosur: http://www.cartillaciudadania.mercosur.int/oldAssets/uploads/Plan de Acción - Anexo declaración Puerto Vallarta.pdf.

MITRE Corporation. (2020, Marzo). *MITRE ATT&CK: Design and Philosophy*. Retrieved Agosto 16, 2021, from http://attack.mitre.org: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf.

Mundo Marítimo. (2021, 04 26). *Mundo Marítimo*. Retrieved from Ciberataques y los frágiles sistemas de seguridad del transporte marítimo: https://www.mundomaritimo.cl/noticias/ciberataques-y-los-fragiles-sistemas-de-seguridad-del-transporte-maritimo.

Nachreiner, C. (2018, 08 18). *Help Net Security*. Retrieved from the security issues 3D printing should solve before going mainstream: https://www.helpnetsecurity.com/2018/08/08/security-issues-3d-printing/.

NATO. (2021, Julio 02). *North Atlanctic Traety Organization*. Retrieved from Cyber Defence: https://www.nato.int/cps/en/natohq/topics_78170.htm.

NIST. (2019, 06 01). *Consideraciones para la gestión de*. Retrieved from https://doi.org/10.6028/NIST.IR.8228es.

OEA. (2016, 10 10). *Organización de Estados Americanos*. Retrieved from Comunicado de prensa C-063/16: https://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-063/16.

OEA. (2008, 08 29). Retrieved from Una estrategia Interamericana integral de seguridad cibernética: http://www.oas.org/juridico/english/cyb_pry_estrategia.pdf.

Perdigón Llanes, R., & Pérez Pino, M. (2020). *Análisis holístico del impacto social de los negocios electrónicos en América Latina, de 2014 a 2019*. PAAKAT: Revista de Tecnología y Sociedad, 10(18), 1-23.

Poulsen, K., McMillan, R., & Evans, M. (2021, 09 30). *The Wall Street Journal*. Retrieved from A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death: https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116.

Rivera Guerrero, Á., Hablich Sánchez, F., & Berni Morán, L. (2018). Dinero Electrónico: Beneficios Tributarios. Revista Global de Negocios, 6(1), 77-92.

Sanger, D. E., & Perlroth, N. (2021, 06 08). *New York Times*. Retrieved from Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity: https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html.

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

Segura Serrano, A. (2017). *Ciberseguridad y Derecho internacional*. Retrieved from https://www.researchgate.net/publication/322943366_Ciberseguridad_y_Derecho_internacional.

Telefónica Tech. (2021, 09 30). Retrieved from Informe de convergencia entre *IoT*, *Big Data* e IA: https://empresas.blogthinkbig.com/informe-covergencia-iot-big-data-ia/.

Terol, M. (2021, 08 04). Retrieved from El Edge Computing y la ciberseguridad: ventajas, retos y desafíos: https://empresas.blogthinkbig.com/ciberseguridad-edge-computing/.

TrendMicro Inc. (2021, 09). *Cyber Risk Index*. Retrieved from https://www.trendmicro.com/es_mx/security-intelligence/breaking-news/cyber-risk-index.html.

United Nations. (2021). *United Nations - Office on Drugs and Crime*. Retrieved 07 30, 2021, from https://www.unodc.org/unodc/es/cybercrime/index.html.

WEF. (2021). *The Global Risk Report, 16th Edition*. Switzerland: World Economic Forum.

_____(2021, Enero 21). *World Economic Forum*. Retrieved 07 23, 2021, from These are the top cybersecurity challenges of 2021: https://www.weforum.org/agenda/2021/01/top-cybersecurity-challenges-of-2021.

Wlodarczak, P. (2017). Cyber Immunity - A Bio-Inspired Cyber Defense System. (S. I. Publishing, Ed.) Retrieved from https://www.researchgate.net/: Cyber_Immunity_-_A_Bio- https://www.researchgate.net/publication/315861769_Inspired_Cyber_Defense_System.

El aprovechamiento de las nuevas oportunidades tecnológicas no constituye simplemente una opción, sino que representa un cambio necesario e ineludible para cumplir con las nuevas expectativas del mercado. En consecuencia, el uso de tecnologías digitales ha experimentado un crecimiento exponencial, facilitando los procesos logísticos y posicionando a los datos como uno de los activos más importantes de las instituciones. Sin embargo, ello ha generado a su vez un aumento del espacio expuesto a riesgos tecnológicos.

En el presente estudio se aborda la problemática de la ciberseguridad en las cadenas de suministros desde el punto de vista de la gestión de dichos riesgos con un enfoque proactivo, por medio de los modelos disponibles para tal fin, desde la perspectiva individual de las tecnologías disruptivas más utilizadas en logística y, finalmente, desde un enfoque institucional y de gobernanza.

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

LC/TS.2022/70