Original: **Español**

www.cepal.org/transporte

número 6 / 2020 / ISSN: 1564-4227

FAL

BOLETÍN 382

FACILITACIÓN, COMERCIO Y LOGÍSTICA EN **AMÉRICA LATINA Y EL CARIBE**

La ciberseguridad en tiempos del COVID-19 y el tránsito hacia una ciberinmunidad

Antecedentes

La seguridad es un bien público regional, en tanto es de interés para toda la sociedad en sus distintas esferas (local, nacional, regional e internacional). En el ámbito logístico, una aplicación sensata de medidas coordinada debidamente con los procesos de facilitación, no solamente reducen los niveles de riesgo y vulnerabilidad de las cadenas logísticas, sino que además contribuyen a incrementar la conciencia respecto al problema de seguridad, ordenan la operación de los terminales de carga, →

El presente *Boletín FAL* se inscribe dentro de las Reflexiones sobre Tecnologías Disruptivas en el Transporte que la CEPAL suele realizar en estas entregas. En esta oportunidad analiza la importancia de la ciberseguridad en el contexto logístico, especialmente en el contexto actual de pandemia.

El documento fue realizado por Rodrigo Mariano Díaz, Consultor de la CEPAL. Para mayores antecedentes sobre esta temática contactar a logisticsandinfrastructure@cepal.org.

NACIONES UNIDAS

CEPAL

propician mejores condiciones operativas e incrementan la eficiencia de los controles de las autoridades. Teniendo en cuenta todos los elementos señalados, se tendrán efectos positivos sobre la competitividad y productividad de la economía (Pérez-Salas, 2013).

Tanto el sector público como privado han desarrollado acciones para fortalecer la seguridad de las cadenas logísticas, como las iniciativas *Customer Trade Partnership Against Terrorism* (C-TPAT), *Container Security Initiative* (CSI), la *Free and Secure Trade* (FAST) y la iniciativa del *Business Alliance for Secure Commerce* (BASC). También deben destacarse, las certificaciones de calidad y seguridad, como la norma ISO 28.000 que es un estándar de carácter transversal que promueve las mejores prácticas en auditoría de riesgos y manejo de eventos de seguridad en la cadena de suministros, como así mismo las adopciones de certificaciones SOLAS y PBIP en el ámbito del transporte marítimo y puertos.

La CEPAL también ha destacado la necesidad de una Política Nacional de Logística que funcione como órgano rector de la actividad, coordine y aglutine las distintas iniciativas internacionales, regionales, nacionales y locales, tanto públicas como privadas, para generar soluciones integrales y eficientes. Esta política debería ser el resultado de la participación de los actores privados, y también debería considerar al menos tres ejes interrelacionados: Facilitación del Comercio, Logística, e Infraestructura, de forma tal de incentivar la apertura de nuevos mercados para las cargas, reducir la brecha de infraestructura, promover la reducción sistemática de los costos logísticos, favoreciendo la innovación e incorporación de tecnología para generar valor, acorde con el paradigma de políticas integradas desarrollada y propiciada por la CEPAL (Jaimurzina, Pérez-Salas y Sánchez, 2015).

Recientemente, también se ha llamado la atención de las autoridades y del sector privado del sector de la logística, sobre los cambios que trae aparejada la 4ta revolución industrial, compuesta por tecnologías como automatización y robótica, *blockchain*, Internet de las cosas, *big data* e inteligencia artificial, entre otras. El sistema logístico del futuro, en consecuencia, apunta a la interconectividad de la información, la optimización del tiempo y los recursos, con una fuerte inversión y desarrollo en innovación para mantener su competitividad. Con el aumento de la tecnología, los ciberataques también se están volviendo más sofisticados a medida que los ciberdelincuentes utilizan diferentes tácticas y tecnología para explotar vulnerabilidades, por lo que la logística deberá aprender a lidiar con este tema y hacerlo parte de su matriz de riesgo, así como lo hizo con otras amenazas en el pasado, como el narcotráfico y el terrorismo. El avance tecnológico exige una nueva mirada al modelo de negocios que existe actualmente. El paradigma del espacio-tiempo es diferente a todo lo conocido algunos años atrás, y lo será mucho más en un corto tiempo. La magnitud de los cambios exige un cambio cultural profundo de la gobernanza logística, especialmente en lo que se refiere a la cooperación pública-privada, la ciberseguridad y la incorporación de objetivos de resiliencia en todos los procesos de la cadena logística (Barleta, Pérez-Salas y Sánchez, 2019).

Dentro del creciente marco de las representaciones digitales y virtuales de los objetos físicos (o en algunos casos el reemplazo de estos) que contempla la transformación digital de los procesos logísticos, es esperable un aumento de la posibilidad de ser afectado por actos ilícitos digitales. En el contexto actual de transformación digital, acelerado a partir del mes de marzo del 2020 con la pandemia causada por el COVID-19, debe considerarse inseparablemente la ciberseguridad, como una parte integral y actualizada de la seguridad física y patrimonial. El estudio *Global Risk Factor* de *World Economic Forum* del año 2020, confirma esta percepción donde los riesgos de ciberseguridad ocupan el segundo lugar detrás de desastres naturales por su probabilidad de ocurrencia e impacto, véase WEF, 2020.

El presente documento busca alertar sobre la importancia de la ciberseguridad dentro del ámbito de la logística, promover acciones de seguridad cibernéticas dentro de ella y un cambio de paradigma de seguridad, transitando el camino desde la ciberseguridad hacia la ciberinmunidad.

I. Cambios en el paradigma de la ciberseguridad

En esta sección se presentan los conceptos principales que forman parte del ámbito tecnológico de la seguridad. Estos conceptos permitirán en las secciones siguientes del documento, interpretar con mayor precisión las estadísticas sobre el estado actual de amenazas de ciberdelito presentes a nivel global, y particularmente en América Latina y el Caribe.

Estos conceptos, además, permitirán interpretar de mejor manera la información procesada de las actividades de ciberseguridad, facilitará el debate entre profesionales de la materia y personas afines a otras especialidades, elevando de este modo la concientización sobre la ciberseguridad.

A. La tríada de la ciberseguridad

Los profesionales de seguridad persiguen tres principios fundamentales a la hora de valorar la protección de la información. Estos son *disponibilidad, integridad y confidencialidad*, elementos conocidos como la tríada CID por las siglas en inglés de:

- Disponibilidad: persigue el objetivo de que la información, los sistemas para procesarla y accederla, las redes de distribución y los equipos necesarios de parte del usuario final, estén al alcance y funcionando correctamente de manera oportuna.
- Integridad: busca que la información permanezca inalterada por procesos o accesos no autorizados, desde su origen hasta su utilización, y a lo largo de todo el ciclo de vida del dato.
- Confidencialidad: establece que la información pueda ser accedida únicamente por los usuarios y procesos con el correspondiente nivel de autorización para hacerlo.

En los análisis de riesgo de ciberseguridad, estos tres principios se evalúan de manera individual para determinar el nivel de exposición a cada uno de ellos. Luego, para cada uno, se utilizan diferentes contramedidas para alcanzar un nivel de riesgo residual admisible. La tríada de seguridad de la información puede debilitarse (o vencerse) mediante diferentes tipos de ataques que se describen a continuación.

B. Descripción de *malware* y sus principales variantes

Malware: Se denomina de esta manera, por los términos en inglés ***mal****icius soft****ware***, a cualquier tipo de código escrito en lenguaje informático, que al ejecutarse realiza acciones dañinas en un sistema de manera intencional y sin el conocimiento del usuario o propietario de dicho sistema. Antes que el término fuera acuñado en el año 1990 por Yisrael Radai, se utilizaba comúnmente el término *virus informático* para referirse a este concepto. En la actualidad, el virus informático, como se explicará luego, es un caso particular de *malware*, que en general sus motivaciones más habituales son:

- Experimentar al aprender.
- Provocar molestias y satisfacer el ego del creador.
- Producir daños a un sistema informático. Estos daños se pueden provocar al *hardware* (por ejemplo, Stuxnet)[1], al *software*, en los datos o generar una indisponibilidad en el sistema completo (por ejemplo, Code Red)[2].
- Provocar una degradación en el funcionamiento del sistema.
- Sacar beneficio económico mediante:
  - Robo de información confidencial (personal, empresarial, de defensa, etc.) para ser utilizada en fraudes posteriores, o ser revendida a terceros. En estos casos el *malware* toma el nombre particular de *spyware*.
  - Rescate solicitado al propietario del sistema, como en el caso del *ransomware* (se explicará en detalle más adelante).
  - Presentación de publicidad no solicitada, llamados *adwares*.
  - La participación involuntaria del sistema en redes ocultas, con fines delictivos, llamadas *botnets*[3].

En términos técnicos, la estructura del *malware* puede contener más de un componente. La porción fundamental corresponde a la carga útil, y es el código malicioso propiamente dicho, por lo tanto, siempre está presente. Puede contener tres porciones adicionales destinadas a distribuir automáticamente la infección, ocultar la funcionalidad verdadera del *malware* (por ejemplo, haciendo creer al usuario que se trata de un protector de pantallas) y finalmente una porción destinada a ocultar la actividad maliciosa (como ejemplo, mediante el borrado de registros de actividad).

El *malware* puede recibir nombres específicos de acuerdo a la función para la que fue creado, o actividad maliciosa que ejecuta, algunas de estas son las siguientes:

- **Virus**: es el tipo de *malware* más común. Se trata de un archivo ejecutable, que al activarse produce el daño para el que fue creado. Tiene propiedades para propagarse dentro del sistema informático en el que fue alojado.
- **Gusano**: es capaz de ejecutarse por sí mismo. Puede propagarse por una red de datos y encontrar vulnerabilidades en otros sistemas, e instalarse en ellos.
- **Troyano**: debe su nombre al Caballo de Troya, y tal como en ese caso, se trata de un programa que parece inofensivo y/o útil, pero tiene una funcionalidad maliciosa oculta. Por lo general, esta funcionalidad permite el control remoto del sistema afectado, o habilita *backdoors*[4] que permiten conexiones no autorizadas que tratan de pasar inadvertidas. Por lo general, no se reproducen.
- **Bomba lógica**: se activa luego de cumplirse una condición. Generalmente, una vez cumplida una cantidad específica de iteraciones, o más comúnmente, una fecha y hora determinada.
- ***Adware***: se encargan de mostrar publicidad no solicitada. Cuando el *adware* tiene por finalidad recaudar dinero de publicidad para financiar aplicaciones gratuitas, recibe el nombre de *shareware*.

[1] Stuxnet es un *malware* que afecta equipos con Microsoft Windows. Es el primero descubierto por atacar equipos industriales, reprogramando los PLCs y ocultando dichos cambios para evitar ser detectado. Stuxnet llegó a ser detectado en ataques a infraestructuras críticas como centrales nucleares.

[2] CodeRed fue un *malware* descubierto en Julio de 2001. El día 19 de julio del mismo año, afectó a 359.000 servidores de *web*.

[3] 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.

[4] 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.

- ***Spyware***: cumple la función de capturar información privada del equipo afectado, y enviarla sin el consentimiento del usuario. Esta información, puede ser de procesos industriales, datos personales, tarjetas de crédito, direcciones de correo electrónico (que luego se utiliza para envío de correo no solicitado), o sobre páginas que se visita. Algunas veces el *spyware* se instala como un troyano, es decir se oculta dentro de otro programa.
- ***Keylogger***: permite guardar en un archivo la totalidad de las teclas pulsadas por el usuario, sin importar en qué aplicación lo haga. De esta manera, el archivo tiene información sensible como contraseñas, chats privados, contenidos confidenciales, etc.
- ***Rogueware***: emula a un producto con fines de protección de seguridad, como antivirus o *antimalware*, indicando al usuario imperiosamente que debe ejecutarse, debido a una supuesta afectación del equipo que se está utilizando[5]. Por lo general, se activan en páginas *web*, y cuando se quiere proceder a desinstalarlo, solicita un pago por su supuesto uso.
- ***Decoy***: imita la interfaz de control de acceso de una aplicación para poder robar información de usuario y contraseña.
- ***Dialer***: casi extinto, debido a los nuevos modos de acceso a Internet mediante WiFi o ADSL, los *dialers* fueron muy populares cuando se accedía a Internet mediante el uso de *modems* telefónicos. Tienen por finalidad marcar de manera no solicitada una línea de teléfono con pago especial, y dejar la línea abierta cargando el coste al usuario infectado.
- ***Wiper***: tipo de *malware* cuya función es borrar información del ordenador donde se ha instalado.
- ***Ransomware***: es un tipo de *malware* que debe su nombre a la unión de los términos *ransom* (rescate) y *software*, y que, al ejecutarse, toma como rehén al sistema afectado mediante un proceso de encriptación, y exige luego pagar por un rescate para recuperar la operatividad de dicho sistema. Demás está decir que pagar un rescate para recibir esta clave, no asegura su recepción, y nunca se debe confiar en el pago como solución a un problema de esta naturaleza.

C. Ataques mediante ingeniería social

La ingeniería social se refiere a los esfuerzos para influenciar ciertas actitudes y comportamientos sociales a gran escala[6], por parte de gobiernos, medios o grupos privados, con el fin de obtener determinados resultados en la población alcanzada. En el

[5] A esta técnica de intimidar al usuario para instalar una aplicación que promete protección se la denomina *scareware*.

[6] Para entender el resultado de la ingeniería social, podemos referirnos a los estudios realizados por el Profesor Robert Cialdini mencionados en su libro *"Influence: The Psychology of Persuasion"* donde concluye que la influencia utilizada para la ingeniería social se basa en los 6 principios fundamentales de reciprocidad, compromiso y consistencia, prueba social, autoridad, simpatía y escasez.

contexto de ciberseguridad, el concepto se utiliza para indicar aquellas acciones orientadas a manipular a las personas para realizar ciertas acciones en un sistema informático, o divulgar información confidencial con fines fraudulentos. Comúnmente los ataques de ingeniería social ocurren por correo electrónico o llamados telefónicos, existiendo algunas otras técnicas. Se clasifican de la siguiente manera:

- ***Vishing***: mediante llamados telefónicos se trata de obtener información de valor de manera encubierta en encuestas, persona o institución de confianza, de forma que la víctima no sospeche que está siendo engañada.
- ***Baiting***: apelando a la curiosidad de las personas y al principio humano que todos quieren ayudar, se deja deliberadamente un dispositivo con información (*pen drive*, DVD, etc.), infectado con un *malware*, en un lugar fácil de encontrar. Cuando la víctima utiliza este dispositivo encontrado para verificar su origen o contenido, el *malware* se instalará, dando paso a las diferentes modalidades descritas para los distintos tipos de *malware*.
- **Pretextos**: es la creación de un escenario ficticio donde la víctima actúa de manera poco común o diferente a como lo haría en circunstancias naturales, revelando de esta forma información de valor o dando lugar a acciones del atacante. Por ejemplo, mediante esta técnica, un ingeniero social podría establecerse en un puesto de trabajo fingiendo ser el reemplazo de una persona o suplantando a una persona legítima.
- **Redes sociales**: si bien las redes sociales nacieron con fines de interacción en círculos de confianza, el uso descuidado o con configuraciones de privacidad incorrectas, se han transformado en las fuentes más peligrosas. Las personas que no dediquen atención a las configuraciones de seguridad o privacidad en las redes sociales pueden dejar al descubierto datos personales sensibles y relaciones, que pueden ser utilizados con fines de perpetrar un ataque dirigido.
- ***Phishing***: es un ataque muy simple y antiguo realizado por correo electrónico, pero de tan alta efectividad que sigue siendo uno de los vectores de ataque más utilizados en la ingeniería social. Consiste en enviar un correo electrónico, que invita a actuar de manera impulsiva dado el sentido de urgencia u oportunidad que logra emular el autor de la correspondencia. En el correo se insta a acceder a un vínculo que emula una página de Internet legal, con usuario y contraseña. De esta manera, la víctima ingresa sus credenciales de acceso reales, que luego quedan en conocimiento del atacante para ser utilizadas en el verdadero sitio. Por lo general, las páginas que se intentan emular corresponden a sitios de pago electrónico, instituciones financieras o sitios de comercio electrónico, por su gran poder de monetización inmediato. Pero no son los únicos casos. Información de identidad o fiscal puede ser objeto de los ataques de *phishing*. La efectividad de este método es tan elevada, que en los últimos tiempos se ha transformado en uno de los tres principales vectores de ataque para enviar accesos a *ransomware*, siendo la víctima quien ejecuta voluntariamente la instalación del *malware*, creyendo que accede a algo de su interés o necesidad, dando lugar a que este posteriormente encripte su sistema.
- ***Quid pro quo***: cuyo significado es "algo a cambio de algo", se denomina al método utilizado en llamadas telefónicas a los empleados de una institución, presentándose como un integrante del soporte técnico, e informando la existencia de un problema real, para luego ofrecer su ayuda para solucionarlo. Una vez el usuario permite esta ayuda, el atacante instala el *malware* en el sistema destino o realiza las verdaderas acciones que motivaron su llamado.

Como se muestra en los cuadros 1 y 2, son las organizaciones con menor cantidad de empleados las que tienen una mayor tasa de recepción de correos electrónicos fraudulentos, en contraposición a la tendencia cultural existente que los ataques afectan principalmente a las grandes compañías.

Cuadro 1
Tasa anual de correos electrónicos maliciosos por tamaño de organización

Tamaño de la organización	Tasa de correo malicioso (1 en)
1-250	323
251-500	356
501-1 000	391
1 001-1 500	823
1 501-2 500	440
2 501+	556

Fuente: Symantec (2019), ISTR - Internet Security Threat Report, Volume 24, Mountain View, USA, February [en línea] https://docs.broadcom.com/doc/istr-24-2019-en.

Cuadro 2
Cantidad de correos electrónicos maliciosos por tamaño de organización

Tamaño de la organización	Usuarios afectados (1 cada)
1-250	6
251-500	6
501-1 000	4
1 001-1 500	7
1 501-2 500	4
2 501+	11

Fuente: Symantec (2019), ISTR - Internet Security Threat Report, Volume 24, Mountain View, USA, February [en línea] https://docs.broadcom.com/doc/istr-24-2019-en.

D. Diferentes modalidades de ataque

En las secciones anteriores, se han revisado las principales modalidades para vulnerar las debilidades derivadas del uso de la tecnología. Partiendo de dichas modalidades, y algunas más específicas que son inherentes a las tecnologías y por ende exceden el espíritu de este documento, la industria llevada adelante por los ciberdelincuentes ha desarrollado a lo largo de los años diferentes técnicas relacionadas con la modalidad de ataque, incluso en el último tiempo acelerada por la tecnología misma y sus avances. El uso de la inteligencia artificial, por ejemplo, ha perfeccionado los principales métodos de ataque que pueden realizarse de manera dirigida, masiva o mixta.

Si bien en los últimos tiempos se han visto muchas víctimas de *ransomware* de distribución masiva mediante técnicas de *phishing*, la industria del cibercrimen ha mejorado sus resultados mediante el uso de una técnica mixta, compuesta por un primer paso con técnicas de descubrimiento masivo de potenciales vulnerabilidades, que una vez descubiertas son explotadas de manera dirigida, usando procedimientos y herramientas tradicionales. También se ha visto un considerable aumento en la personalización de los contenidos utilizados en las técnicas de ingeniería social, mediante la explotación de datos filtrados en eventos relacionados con fuga de información. Durante el año 2019, se comenzó a utilizar información filtrada de usuarios y contraseñas de sitios vulnerados, para alimentar el contenido de correos extorsivos. En estos correos, el atacante declara poseer contenido ilícito del destinatario y conocer el usuario y contraseña enviadas al correo electrónico. Dado que en muchos casos las personas utilizan la misma contraseña para múltiples sitios, la contraseña enviada puede resultarle familiar a la víctima, y por consiguiente se siente desconcertada frente a la posible existencia de un contenido de estas características. Por supuesto que el atacante sólo tiene el usuario y contraseña, y está construyendo un relato falso basado en esta debilidad del uso de contraseñas idénticas para muchos sitios. Es alarmante la cifra revelada por IBM, donde se contabilizan 8.500 millones de registros de datos personales robados durante el año 2019, que luego son comercializados o intercambiados en las redes de ciberdelincuencia, para ser monetizados de manera

instantánea o utilizados como información para construir ataques de ingeniería social. Estos datos se ofrecen e intercambian en la misma red y con las mismas conexiones donde ocurren nuestros intercambios habituales de Internet. Solo que subyacen en diferentes modos de acceder, y se ocultan a los usuarios y a los métodos de uso y descubrimiento habituales. Si bien comparten el medio, no tienen el mismo fin, dando lugar a diferentes niveles de complejidad para acceder a sus contenidos.

E. *Deep web*, *Dark web* y *Marianas web*

Para referirse a los conceptos del contenido que no es visible, se debe antes hacer una referencia a la totalidad del contenido de Internet. A esta totalidad se la suele representar como un iceberg, donde se asocia a la parte visible con la proporción del contenido que es visible en la Internet tradicional, que es la *web* tal como la conocen la mayoría de los internautas, por lo que también se la denomina *surface web*. La *surface web* está formada por contenido que los buscadores como Google, Yahoo, Bing, entre otros, indexan y ofrecen a los usuarios mediante una búsqueda similar a un directorio telefónico. Pero, siguiendo con la analogía del iceberg, gran parte del contenido de Internet, no se indexa para ofrecerse a los usuarios ya que tiene información técnica que requiere de la *surface web* para ser utilizada. Entran dentro de este segmento las bases de datos donde se realizan búsquedas, los correos electrónicos que almacenan los proveedores de este servicio, etc. A todo el contenido de Internet que no está indexado, y por lo tanto no es visible, se lo denomina *deep web*. Es por ello que muchas veces a la *deep web* se la llama también *invisible web* (*web* invisible) o *hidden web* (*web* oculta).

Dentro de esta porción oculta, que representa aproximadamente un 90% del contenido y que no es accesible de manera transparente a los internautas, hay una pequeña porción que solo puede accederse mediante aplicaciones específicas, es decir, una porción de aproximadamente el 0,1% del contenido, que intencionalmente se oculta del uso habitual de la red. Esta porción, que inicialmente se trataba sólo de algunas páginas llamadas *darknets*, es la que actualmente lleva el nombre de *dark web*. Para acceder al contenido de la *dark web*, se utiliza específicamente una de ellas llamada TOR, por las siglas de *The Onion Router* (el enrutador cebolla). Este proyecto tiene por objetivo crear una red de comunicaciones distribuidas y superpuestas a la red convencional, y proveer el punto de acceso al resto de las páginas que forman la *dark web*, las que se han ocultado intencionalmente por su contenido ilícito, siendo éstas páginas lugares donde habitualmente los ciberdelincuentes ofrecen sus servicios y productos; registros obtenidos en fugas de datos tales como tarjetas de crédito, números de pasaportes, correos electrónicos con sus respectivas contraseñas, servicios de ataques dirigidos a instituciones y empresas, como también páginas destinadas al tráfico de drogas, trata de personas y ventas de armas, entre otros contenidos ilícitos.

Existe un nivel aún más profundo y oculto en la *deep web* que por analogía con la fosa del mismo nombre, se la llama *Marianas web*, y el acceso está limitado a un segmento muy pequeño de hábiles programadores a través del uso de complejos algoritmos. El contenido ilícito que puede encontrarse en estos casos es de sensibilidad extremadamente peligrosa.

II. Incidentes recientes y datos estadísticos de ciberseguridad ocurridos en la industria logística

El conocimiento de diferentes hechos ocurridos, las problemáticas, y sus frecuencias o probabilidades de ocurrencia, permiten determinar la probabilidad que luego se ha de utilizar en los análisis de los riesgos relacionados con la tríada de la seguridad, que cada proceso enfrenta en la actualidad. Desde 2011 y hasta 2013, el Puerto de Amberes en Bélgica, fue víctima de un ataque encargado por un cártel de droga contra sistemas informáticos de la terminal con el fin de liberar contenedores sin que las autoridades portuarias lo notaran. Al descubrirse el ataque, se incorporaron dispositivos de seguridad electrónica para proteger el perímetro de la red del puerto, pero estos fueron nuevamente vulnerados y se logró continuar

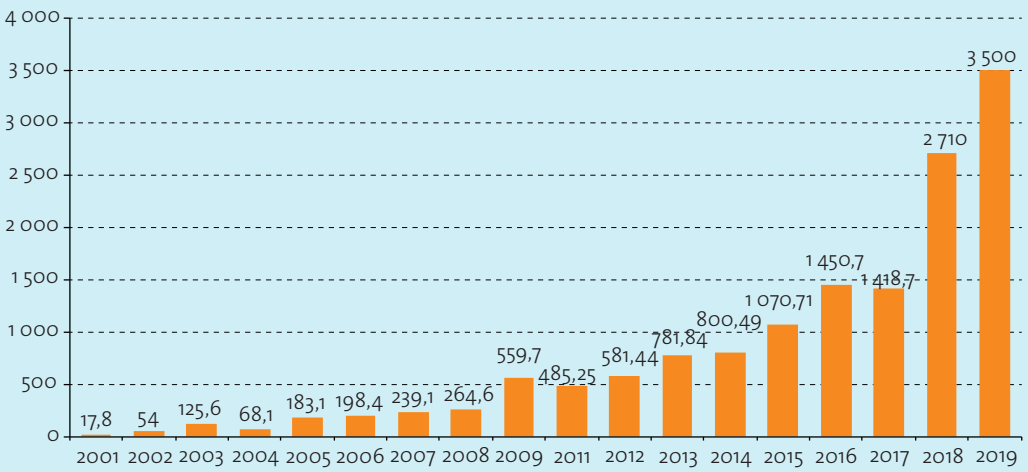
con las acciones del ataque. Se incautaron en este incidente, drogas ilícitas y contrabando por un valor aproximado de 365 millones de dólares además de armas de fuego.

En junio de 2017, la naviera MAERSK sufrió un ataque de *ransomware* que provocó una disrupción operativa que le generó pérdidas por USD 264 millones. La investigación de este incidente arrojó que la infección sufrida se debió a la instalación de un *software* no controlado en la laptop de un empleado del área comercial en Ucrania. En Julio de 2018, el puerto de San Diego en Estados Unidos fue atacado también por un *ransomware* con una pieza de *software* que provocó disrupciones administrativas y en la obtención de permisos de uso de puerto. Más tarde, el mismo año, COSCO fue atacado con disrupciones operativas en su sede de Estados Unidos de Long Beach. En septiembre de 2018 el puerto de Barcelona, en España fue víctima de ataques de *ransomware*, provocando disrupciones en tareas administrativas, sin tener información económica de estos daños. Durante febrero de 2019 se informaron ataques de *GPS jamming* en guardacostas de la marina de Estados Unidos en el puerto de New York, y en julio frente al puerto de Shanghai. Recientemente se reportó un caso que afectó a la naviera MSC, provocado por una pieza de *software* maliciosa que produjo una disrupción en los sistemas de desintermediación denominados MyMSC afectando el acceso a los servicios por parte de los clientes finales.

Las pérdidas económicas por ataques de ciberseguridad se acrecientan en la medida que la digitalización de los procesos avanza, tal como muestra el gráfico 1. Es importante, tener presente que estas cifras contemplan únicamente los eventos denunciados, aunque se sabe que muchos de los incidentes ocurridos no son reportados para no dañar la reputación de la compañía y son tratados de manera privada.

Gráfico 1

Mundo: pérdidas económicas anuales debido al cibercrimen
(En millones de dólares)



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

Suele pensarse que los ataques de ciberseguridad ocurren en menor grado en América Latina y el Caribe, dada la escala de las organizaciones y porque existe un menor grado de utilización de nuevas tecnologías en comparación con otras regiones del mundo. Sin embargo, un estudio reciente de CheckPoint de julio de 2020, muestra que la región presenta las mismas probabilidades de ser atacada que otras regiones del mundo, destacándose incluso que algunos países como Colombia, Bolivia (Estado Plurinacional de), Ecuador, México, Nicaragua, Perú y Venezuela (República Bolivariana de) se encuentran por encima de la media. De igual forma, el mapa en tiempo real de amenazas del laboratorio de la firma Kaspersky, muestra que los países de la región se ubican dentro del primer 25% de los países más atacados en el planeta, destacándose el caso particular de Brasil, que es el tercer país a nivel mundial en ataques registrados.

Estas estadísticas incluyen a las empresas e instituciones relacionadas a la logística y al transporte, rubro que durante el año 2019 mostró una tasa de crecimiento interanual del 78% en los ataques que involucran a diferentes integrantes de las cadenas de suministro, ubicándose de esta manera en el tercer lugar, con un 10% del total de los ataques a nivel global. Este lugar para logística y transporte, que además se mantiene a lo largo de los años entre los primeros, realza el creciente valor de los datos de este sector para la industria del cibercrimen. Se explica esta ubicación, por detrás de mercados financieros y *retail*, debido al valor de los activos electrónicos y la posibilidad de manipular los datos de las cadenas de distribución, esto sin contar con el efecto dominó en el resto de los sectores y en otros servicios, lo cual potencia y multiplica los daños provocados por los incidentes.

El sector de la logística y el transporte, representan también un gran atractivo por el acceso a activos de alto valor para el espionaje entre Estados, como por ejemplo la información biográfica, números de pasaporte, programas de viajeros frecuentes, datos de tarjetas de crédito, itinerarios de viajes, manifiestos de embarque, entre otros elementos que suelen manejarse en la industria.

Respecto al tipo de técnicas utilizadas para vulnerar las instalaciones, los tres principales vectores de ataque inicial corresponden a: el 31% de casos a *phishing*, 30% a escaneo y explotación de vulnerabilidades y 29% a robo de credenciales de acceso. Llama la atención, que la mayoría de los ataques que aprovechan vulnerabilidades existentes en los sistemas de *hardware* o *software*, se tratan de CVE[7] con hasta 2 años de vigencia, es decir se trata de vulnerabilidades de conocimiento público. Más del 80% de los ataques realizados en el primer semestre de 2020, se podrían haber evitado aplicando parches de actualización que se encuentran disponibles desde 2017 o antes, muchos de los cuales son gratuitos. Esto denota no solo la dificultad de estar al día con las actualizaciones de seguridad que proveen los fabricantes de *software*, a pesar de las grandes campañas que ellos realizan y la concientización que recibe el personal técnico de los departamentos de tecnología sobre esta problemática, sino también lo difícil que resulta, en algunos casos, el reemplazo de versiones de *software* obsoleto, por compatibilidad de productos o aplicaciones con sistemas operativos de base en las computadoras de usuario final y en los servidores de procesamiento central.

Además, existe una tendencia errónea a interpretar que resulta más dificultoso, o que no hay tantas herramientas desarrolladas para explotar vulnerabilidades del *hardware* por un tercero. Esto hace muy complejo el reemplazo de ciertos productos de *hardware*, como PLCs o HMIs, que han sido entregados llave en mano en instalaciones industriales, y cuyo reemplazo requiere una reingeniería e inversión. Por este motivo, sumado a la necesidad de contar cada vez más con datos en tiempo real que ha derivado en la conexión de las redes tradicionales de piso de planta o redes industriales, es que los ciberdelincuentes han incorporado a sus herramientas la posibilidad de llegar a este tipo de redes e infraestructura teniendo como objetivo la disrupción operativa.

Es importante mencionar la alta incidencia que tienen las infraestructuras críticas que administran gobiernos e instituciones públicas y privadas en la cadena de logística y en la vida cotidiana de las personas, y es menester de estas organizaciones reparar en los ciberataques que pueden afectar seriamente la economía derivada de actividades dependientes. En este sentido, el informe de X-Force, demuestra una tasa interanual de ataques a redes de OT entre octubre de 2018 y octubre de 2019 de un 2000%. De hecho, la actividad de 2019 supera a la totalidad de los 3 años anteriores. La mayoría de estos ataques responden a vulnerabilidades conocidas de los sistemas SCADAS[8] y ataques de fuerza bruta con contraseñas de fábrica de los sistemas de control industrial o ICS. Avala este hecho, el estudio que realizó Symantec, donde casi el 60% de las contraseñas utilizadas

[7] Las Vulnerabilidades y exposiciones comunes (en inglés, Common Vulnerabilities and Exposures, sigla CVE), es una lista de información registrada sobre vulnerabilidades de seguridad conocidas, en la que cada referencia tiene un número de identificación CVE-ID, descripción de la vulnerabilidad, qué versiones del *software* están afectadas, posible solución a la falla (si existe) o cómo configurar para mitigar la vulnerabilidad y referencias a publicaciones o entradas de foros o blogs donde se ha hecho pública la vulnerabilidad.

[8] SCADA, acrónimo de Supervisor y Control And Data Acquisition (Supervisión, Control y Adquisición de Datos), es un concepto que se emplea para realizar un *software* para ordenadores que permite controlar y supervisar procesos industriales a distancia.

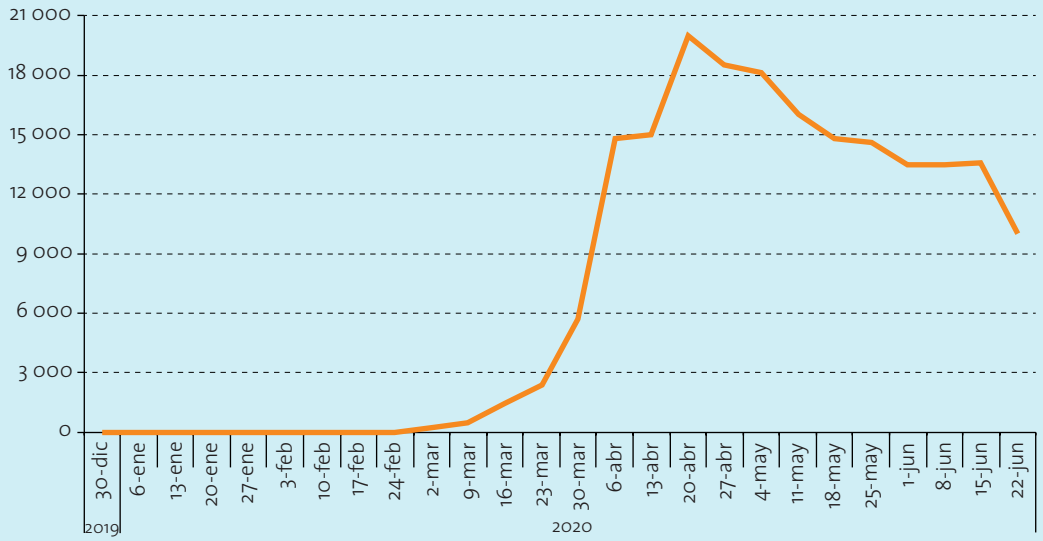
en ataques a redes de OT son triviales y más del 90% de ellos fue realizado con protocolo de red inseguro y de transmisión de datos en texto plano utilizando servicio de telnet. A modo de ejemplo, la contraseña "123456" y "(vacía)" fue utilizada exitosamente en un 24,6% y 17% de los ataques de IOT (Anual) respectivamente, siendo el protocolo telnet a través del cual se reciben el 90,9% de los ataques.

A este contexto complejo que se venía experimentando en ciberseguridad, con la llegada del año 2020, aparece el COVID-19 y se transforma en el agente catalizador de la transformación digital, acelerando la adaptabilidad que los seres humanos venían teniendo a las nuevas formas de trabajo. Junto con su llegada, y con la urgencia de información y distribución de novedades, el *phishing* acompañado de *ransomware* relacionado con el COVID-19 aumentó de forma exponencial, tal como se muestra en el gráfico 2.

Gráfico 2

Mundo: ataques cibernéticos a partir de la llegada del COVID-19

(En número de ataques semanales)



Fuente: CheckPoint (2020), "Cyber attack trends: 2020 mid-year report", Check Point Software Technologies Ltd., Tel Aviv, Israel, Julio [en línea] https://research.checkpoint.com/2020/cyber-attack-trends-2020-mid-year-report/.

Entre junio de 2019 y junio de 2020, una tasa interanual de crecimiento de 108% para ataques de *ransomware* y 833% para ataques a redes de IoT. Este crecimiento refleja la explotación de vulnerabilidades expuestas debido a la velocidad con la cual los departamentos de tecnología tuvieron que cubrir una demanda inesperada para disponibilizar la información con nuevos métodos, para más personas y en plazos muy cortos, y de esa manera, lograr mantener los procesos operativos en marcha.

Finalmente, un dato respecto a los ataques de *ransomware* que abre una preocupación nueva y un enfoque diferente, es el caso de una importante firma global de administración de dinero de viajeros que sufrió un ataque de *ransomware* en enero de 2020 y aplicó sus procedimientos de recuperación, negándose a pagar el rescate de la información secuestrada, fue amenazada por el grupo creador del Sodinokibi a divulgar 5 Gb de información de clientes robada previa a la encriptación, exponiéndolos de esta manera a un posible incumplimiento de las leyes internacionales de protección de datos personales de la Unión Europea (GDPR)[9].

[9] El Reglamento General de Protección de Datos (GDPR) (Reglamento 2016/679) es un reglamento por el que el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión Europea tienen la intención de reforzar y unificar la protección de datos para todos los individuos dentro de la Unión Europea (UE).

III. Principales desafíos de ciberseguridad para el transporte y la logística en América Latina y el Caribe

De la interpretación de las estadísticas presentadas, en relación con la evolución de los ataques en cantidad y en formato, la CEPAL determina los principales desafíos para el futuro cercano en materia de ciberseguridad, dentro de las actividades relacionadas con el transporte y la logística. Se sostiene en las personas que integran la operación de las empresas e instituciones que forman el ecosistema logístico, la tendencia cultural a subestimar los problemas de ciberseguridad, a pesar del crecimiento de estos durante los últimos años. Esto se deduce de problemáticas que se relacionan con el comportamiento habitual de los individuos. El *phishing* y las contraseñas débiles son las causas iniciales de dos tercios de los ataques, y el último tercio debe su origen a la falta de conciencia en la necesidad de mantener los sistemas actualizados. Por lo tanto, el factor humano sigue siendo determinante en los desafíos actuales, y principalmente, en capital humano ajeno a las áreas de tecnología. Entender esta problemática es clave, ya que el desarrollo de estrategias en relación con este desafío no solo beneficiaría a las actividades laborales, sino también al cambio de paradigma de la seguridad de toda la sociedad tal como se conoce hasta hoy, agregando su nueva dimensión indispensable de la ciberseguridad.

Se puede percibir, por los tiempos que se demora en reaccionar a actualizaciones y por la falta de políticas internas para renovar equipos que van quedando sin soporte del fabricante, que se sigue viendo a la seguridad como un proceso diferenciado (o secundario, cuando no inexistente) de la innovación tecnológica, lo cual representa mayores costos internos y esfuerzos operativos a la hora de prevenir o corregir los riesgos tecnológicos relacionados con uno o más de los componentes de la tríada de la seguridad.

En el año 2020 existirán 4 veces más dispositivos conectados a Internet que personas en el planeta, 31.000 millones de dispositivos estarán entregando datos en tiempo real para ser utilizados dentro de los ecosistemas de *big data* e inteligencia artificial. Sumando esta información a la proveniente de otras tecnologías, desde este año 2020 hasta el año 2025, se va a generar 4 veces más información que en toda la historia de la humanidad. Este crecimiento en la superficie de posibles ataques propiciará el crecimiento de la actividad delictiva sobre los datos y dispositivos del ecosistema logístico.

A pesar de esta perspectiva, la oportunidad de que los estados de América Latina y el Caribe puedan beneficiar sus servicios logísticos con la implementación de nuevas tecnologías participantes de la logística 4.0, no puede verse afectada, ni mucho menos desanimada, por los desafíos de ciberseguridad. Se debe recordar que el peor riesgo tecnológico no radica en la ciberseguridad, sino en la falta de innovación y en no explotar las oportunidades de mejoras de eficiencia en las cadenas logísticas mediante la utilización de nuevas tecnologías, y que el estado actual de la ciberseguridad, deviene de haber desatendido esta problemática de manera sistemática durante muchos años, pero que en caso de vivirse a la ciberseguridad como un proceso integral en la innovación, no sólo minimiza la exposición al riesgo, sino que también acelera los procesos de cambio y maximiza la eficiencia y confiabilidad de la cadena de extremo a extremo. Por lo cual, es menester comenzar con planes de acción de manera inmediata para minimizar los riesgos tecnológicos, ya que, de otra forma, estos se convertirán en un importante enemigo del desarrollo de la logística 4.0 y, por consiguiente, de la economía derivada de esta importante actividad en los países que componen la comunidad de América Latina y el Caribe.

IV. Plan de acción para asegurar el camino a la logística 4.0

En una economía mundial con cifras de recesión históricas como consecuencia de la pandemia desatada por COVID-19, la industria de ciberdelito mantiene su valor lucrativo y se muestra en creciente actividad. Es imperativo entonces, desarrollar un plan estratégico que permita alinear acciones que estén de acuerdo con la escala del problema.

Tratándose de un tema que escapa a las dimensiones del espacio tradicional de la seguridad física y trasciende fronteras internacionales, es menester fortalecer la cooperación entre naciones y organismos públicos y privados para las investigaciones de ciberdelitos, de manera que se puedan crear organismos y políticas capaces de abordar la problemática de ciberseguridad coordinado globalmente.

En este sentido, existen importantes esfuerzos realizados para mejorar la seguridad logística, como las recomendaciones de seguridad realizadas por la OMI[10], las que tienen su base principalmente en el estándar internacional ISO/IEC 27001 de aplicación general para las tecnologías informáticas y de comunicaciones.

El escaso nivel regulatorio de los países en estas materias, puede afectar la efectividad de estas medidas. Es oportuno entonces, que las oficinas públicas analicen el beneficio que obtendrían sus economías si la actividad fuese regida por normas de cumplimiento similares a las existentes en el rubro financiero. Esta acción administrativa fortalecerá la confianza de los mercados internacionales en la sustentabilidad de la actividad. Sin esta medida, los esfuerzos y recomendaciones que se expresan a continuación dependerán de la voluntad y deber hacer de cada integrante, que seguramente lo harán en beneficio propio, pero seguirán dependiendo del mismo deber hacer y voluntad de sus contrapartes, para la sustentabilidad de su propio proceso y el beneficio de las economías regionales.

A. Ejes de acción del plan estratégico

Siguiendo las recomendaciones del estándar internacional ISO/IEC 27001, es conveniente orientar las acciones generales en 3 ejes principales de acción: Procesos, Tecnología y Personas. Para ello se han seleccionado del mismo, las acciones concretas que permitirán dar los pasos fundamentales en estas directrices.

1. Acciones basadas en los procesos

El abordaje inicial de los procesos debe enmarcarse en una política general que exprese claramente el compromiso con la ciberseguridad de la entidad de mayor jerarquía en la organización, expresando claramente los motivos generales por los cuales la institución considera importante el abordaje de la problemática de manera integral y la debida adhesión de todos los integrantes de la institución.

- La política general es el documento fundacional de un *Sistema de Gestión de Seguridad Informática* que deberá **contener** los documentos de políticas y procedimientos necesarios para las acciones específicas de seguridad.
- Con la mirada en las tecnologías disruptivas, es esencial **considerar** las actividades oportunas de ciberseguridad desde el momento inicial en cada proyecto de transformación digital, entendiendo que cada etapa tiene actividades de ciberseguridad inherentes a las definiciones y entregables de dicha etapa. Cuanto más se demore en pensar en ciberseguridad, más complejo será administrar el riesgo.
- **Desarrollar** un plan de contingencia que permita mantener activos los procesos esenciales de la institución ante posibles incidentes que atenten contra la disponibilidad de la tecnología. El plan debe ser un documento vivo y de mejora continua. El ejercicio habitual y las mejoras no solo fortalecen la confianza en la reacción ante incidentes

[10] Véase MSC-FAL.1/Circ.3 Directrices sobre la gestión de los riesgos cibernéticos marítimos.

reales, sino que se transforma en un verdadero entrenamiento continuo. De la misma manera, el plan de contingencia entrega una lista de mejoras a ejecutar y chequear en su próxima prueba, generando de esta manera un proceso circular de mejora continua.

- **Someter** a los sistemas a pruebas de stress de terceros de manera regular. Hay que estresar permanentemente los sistemas de ciberseguridad con pruebas de tipo hackeo ético o *Penetration test* (*Pentest*) para detectar cambios no controlados y nuevas exposiciones descubiertas, corregir desvíos y luego volver a comenzar. La importancia de este proceso radica en la objetividad con la que un equipo profesional especializado puede detectar desvíos de estándares, o vulnerabilidades, que pueden estar originados, intencionalmente o no, por el funcionamiento, integración, mantenimiento y proyecto inadecuados de los sistemas.
- **Evaluar** la contratación de una póliza de seguro que contemple la transferencia de riesgos de ciberseguridad.

2. Acciones basadas en la tecnología

- Las tareas tradicionales de la seguridad básica de sistemas de información deben ser objetos fuera de discusión y todas deben implementarse. **Hacer respaldos y verificar su utilidad de recuperación**, utilizar protecciones del perímetro lógico mediante el uso de *firewalls* y el uso de antivirus actualizado siguen siendo medidas absolutamente necesarias. Entre el respaldo y la información perdida en un incidente, existe un tiempo al que se ha llamado RPO (*Recovery Point Objective*) y que se debe asumir como la peor condición de restauración. Los procesos dinámicos actuales, no pueden recurrir a esta alternativa de manera frecuente, pero siguen siendo la mejor manera de tener bajo control la peor situación de recuperación de datos, por ejemplo, en el caso de ataque de *ransomware*.
- Gran cantidad de los ataques que se producen, ocurren con equipamiento adecuado e instalado, pero implementado de manera incorrecta y sin revisión de especialistas. Al momento de elegir una tecnología para protección de riesgos específicos, se debe **contemplar** el costo total de propiedad de la solución. Esto incluye el costo de adquisición, el costo y la disponibilidad local del soporte técnico adecuado para su configuración y mantenimiento, y el tiempo en que el producto llega al final de su ciclo de vida, determinando su máxima amortización. Resulta pertinente destacar que es mucho más efectiva una tecnología de evolución intermedia con una implementación correcta, que la tecnología más avanzada sin control de implementación.
- **Actualizar** permanentemente *software* y *hardware*, y mantenerlos dentro de la vigencia del ciclo de vida y con soporte del fabricante. En 2019 se revelaron 150,000 vulnerabilidades. Parchear vulnerabilidades sigue siendo un problema para muchas organizaciones y los cibercriminales lo saben. Más lo será si no se cuenta con soporte del fabricante. Resulta una buena estrategia tener controles por oposición de interés entre áreas que se ocupen de aplicar los parches y el control de estado de estas actualizaciones. Este control puede realizarse con reportes de interpretación simple que permitan, en organizaciones con estructuras reducidas, asignar esta tarea a las áreas de control interno o administrativos, por ejemplo.
- **Contar** con herramientas de análisis avanzado de eventos con alertas on line 7x24x365. Idealmente contar con un proceso de identificación y comunicación que asegure que un incidente de ciberseguridad se atienda inmediatamente para minimizar el impacto. Los responsables de ciberseguridad de las instituciones que han sido víctimas de ataques efectivos destacan la importancia de detectar y aislar rápidamente el ataque y los sistemas afectados. Este proceso puede ser atendido por tecnologías en formato de *software* como servicio, o implementarse con atención humana. En este último caso se lo denomina *Security Operations Center* (SOC), y es una tendencia muy marcada en la actualidad, debido a la velocidad con la que se atiende un incidente cuando este proceso se encuentra implementado.
- Tecnologías intrínsecamente seguras. La mayoría de las tecnologías de negocio nacieron y evolucionaron sin contemplar al mundo hiperconectado. Sistemas Cobol, SAP,

Sistemas de piso de planta, etc., fueron pensados para entornos de redes controladas y de baja interoperabilidad con redes desconocidas. Se viene realizando mucho esfuerzo por agregarles la capa de seguridad necesaria para ser utilizados en los entornos actuales. En los nuevos desarrollos de innovación, se debe **considerar** seriamente el uso de tecnologías intrínsecamente seguras, como por ejemplo el caso de *blockchain*.

- **Contemplar** la utilización de métodos de autenticación de doble factor que eviten los accesos no autorizados derivados del uso de contraseñas débiles.
- **Aplicar** en las redes de tecnología operacional un modelo de defensa en capas para evitar que un ataque provocado en la red de uso administrativo o de gestión pueda expandirse, logrando detener los procesos productivos.

3. Acciones dirigidas a las personas

- Capital humano en general. **Entrenar** a todo el personal de manera permanente. Esta capacitación debe hacerse con entrenamientos de inducción adecuada cuando la persona se incorpora al equipo de trabajo, y debe reforzarse con periodicidad aproximada de 2 años. Debe incluirse en ella, al menos, las políticas de privacidad de los datos, respaldo de información, uso de contraseñas y uso responsable de Internet. Este entrenamiento, además, debe reforzarse mensualmente con capacitaciones cortas que realicen una concientización permanente sobre contraseñas, *phishing*, etc., y es muy conveniente realizar *phishings* éticos y controlados para poder medir la efectividad de la concientización.
- Contar con una copia firmada por cada colaborador de un compromiso de no divulgación que explique claramente los objetivos del mismo y las sanciones por incumplimiento.
- El personal de las áreas de tecnología debe contar con espacios recurrentes asignados a novedades de ciberseguridad para la toma de conciencia.

V. El camino de la Ciberseguridad a la Ciberinmunidad

Durante muchos años, en el ámbito de la ciberseguridad se ha hablado del concepto de miedo, incertidumbre y duda (FUD, por las siglas en inglés de *fear*, *uncertainty, doubt*) el cual ha ayudado a la implementación de tecnologías en materia de seguridad de la información. El detalle que se debe entender respecto al éxito de este concepto es que, en un mundo donde la tecnología de la información creaba sistemas aislados, o conectados a través de puntos específicos con otros sistemas, la utilización de sistemas de defensas como antivirus, *firewalls*, etc., eran la solución a los problemas principales de seguridad electrónica y robo de información confidencial. Durante los últimos años, con el advenimiento de las tecnologías que forman el entorno de trabajo denominado Industria 4.0, en un mundo hiperconectado donde los sistemas han pasado a formar ecosistemas, seguir utilizando el principio FUD, sería un error que podría profundizar la crisis. Esto porque este enfoque podría acrecentar la desigualdad tecnológica entre quienes implementan estos cambios y quienes no los realizan, dejando fuera de la 4ta Revolución Industrial a aquellas instituciones que por miedo no implementan soluciones tecnológicas como *driver* de eficiencia operativa. No correr riesgos tecnológicos, es el mayor riesgo que puede enfrentarse en un mundo hiper-digitalizado y conectado.

Reconociendo que el riesgo nunca puede ser nulo[11], 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 nuestra seguridad es sólo cuestión de tiempo. Por tal motivo, es conveniente comenzar a desarrollar planes estratégicos para que, de forma similar a la que los seres vivos se defienden de ataques a su organismo, los ecosistemas informáticos cuenten con

[11] La definición de riesgo es la función directa del daño potencial de una amenaza o peligro, y la probabilidad de ocurrencia de estos.

un sistema de ciberinmunidad[12]. Un sistema de estas características, al igual que en los organismos vivos, contempla que los sistemas inmunes 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 se adaptan y aprenden, 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 de ataque. Pensar en ciberinmunidad, permitirá en caso de ser abatidos por una amenaza, recuperar rápidamente las funciones operativas esenciales de la institución, permitiendo achicar, de esta manera, el triángulo de pérdidas de la curva de resiliencia, y recuperar rápidamente las funciones habituales, superando eventualmente los resultados previos al incidente.

VI. Conclusiones

En un mundo cada vez más digital y conectado, con tecnologías disruptivas y tiempos de implementaciones muy exigentes, la exposición a recibir un ciberataque es solo una cuestión de tiempo. El esfuerzo debe realizarse entonces para reducir las posibilidades de ocurrencia, mediante un plan de gestión de ciberseguridad, que contemple medidas efectivas sobre los procesos, la tecnología y las personas, independientemente del tamaño de la organización, y al mismo tiempo, prepararse de la mejor manera posible para atender una incidencia.

Es propicio entender al proceso de la ciberseguridad como un sistema inmune similar al biológico, que está compuesto de una serie de elementos con funciones muy diferentes que evitan que se contraiga una infección o enfermedad. De la misma manera que ocurre en los organismos vivos, el sistema inmune de una organización nunca es perfecto, y los virus y otros microbios patógenos encuentran modos de engañarlo o incluso de atacarlo. Sin embargo, los sistemas inmunes comparten un rasgo muy importante: aprenden y se adaptan. Pueden ser "educados" a través de la vacunación contra amenazas potenciales. En tiempos de peligro, pueden ser asistidos con anticuerpos preparados. Mediante algunas técnicas como la de atención inmediata a eventos atípicos detectados por el monitoreo permanente de la actividad tecnológica, las organizaciones pueden defenderse de ciberataques, incluso sin saber muy bien de qué se trata lo que está ocurriendo.

Con este nuevo enfoque llamado ciberinmunidad, la comunidad logística de América Latina y el Caribe puede protegerse individualmente manteniendo la continuidad operativa y la protección de los datos, en el entorno de la logística 4.0. Sin embargo, dado la interdependencia funcional de la cadena logística, la indisponibilidad de uno de sus integrantes afecta a todo el ecosistema, no se puede descuidar ni demorar el desarrollo de organismos y mecanismos regulatorios, que formalicen y fortalezcan la confianza entre los integrantes del sistema de extremo a extremo, y, por lo tanto, mejoren la competitividad y confianza de los mercados globales.

VII. Bibliografía

American Journal of Transportation, AJOT (2019), "U.S. Coast Guard warns of cyber-attack & electronic interference threats to commercial vessels", *Maritime News*, Ajot, August [en línea] https://www.ajot.com/insights/full/ai-u.s-coast-guard-warns-of-cyber-attack-electronic-interference-threats-to-commercial-vessels.

Baker, J. (2020), "MSC confirms website shutdown caused by cyber attack", *Maritime Intelligence*, Lloyd's List, April [en línea] https://lloydslist.maritimeintelligence.informa.com/LL1131957/MSC-confirms-website-shutdown-caused-by-cyber-attack.

[12] El concepto fue elaborado por primera vez por el Profesor Peter Wlodarczak, de la Universidad de Southern Queensland, en su nota técnica llamada "Cyber Immunity - A Bio-Inspired Cyber Defense System".

Barleta, E. P., G. Pérez S. y R. Sánchez (2019), "La revolución industrial 4.0 y el advenimiento de una logística 4.0", *Boletín FAL* 375, número 7, CEPAL, Naciones Unidas, Santiago.
Bateman, T. (2013), "Police warning after drug traffickers' cyber-attack", *BBC News*, October [en línea] https://www.bbc.com/news/world-europe-24539417.
BBC News (2018), "San Diego port hit by ransomware attack", Octubre [en línea] https://www.bbc.com/news/technology-45677511.
CheckPoint (2020), "Cyber attack trends: 2020 mid-year report", Check Point Software Technologies Ltd., Tel Aviv, Israel, Julio [en línea] https://research.checkpoint.com/2020/cyber-attack-trends-2020-mid-year-report/.
Cialdini, R. B. (2006), *Influence: The Psychology of Persuasion*, Harper Collins, USA, ISBN: 006124189x, ISBN-13: 978-0-061241-89-5.
FBI (2020), 2019 *Internet Crime Annual Report*, Federal Bureau of Investigation, US Department of Justice, USA [en línea] https://pdf.ic3.gov/2019_IC3Report.pdf.
IBM Security (2020), IBM X-Force Threat Intelligence Index, IBM, Armonk, USA, febrero [en línea] https://www.ibm.com/security/data-breach/threat-intelligence.
ISO/IEC (2018), "Information technology — Security techniques — Information security management systems — Overview and vocabulary", ISO/IEC 27000: 2018, International Organization for Standardization, Geneva, Switzerland [en línea] https://www.iso.org/standard/73906.html.
Jaimurzina, Azhar, G. Pérez-Salas y R. Sánchez (2015), "Políticas de logística y movilidad para el desarrollo sostenible y la integración regional", *Serie Recursos Naturales e Infraestructura*, Nº 174 (LC/L. 4107), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), noviembre.
Kaspersky (2020), *Ciberamenaza mapa en tiempo real*, [en línea] https://cybermap.kaspersky.com/es/.
La Vanguardia (2018), "El Puerto de Barcelona sufre un ciberataque que podría retrasar la entrega de mercancías", Barcelona [en línea] https://www.lavanguardia.com/local/barcelona/20180920/451930581288/puerto-barcelona-sufre-ciberataque-y-podria-causar-retraso-entrega-mercancias.html.
Mathews, L. (2017), "Not Petya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million", *Forbes*, Agosto [en línea] https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/#6a6794f64f9a.
Moiseev, A. (2019), "Di sí a la ciberinmunidad y no al miedo", Kaspersky Lab [en línea] https://www.kaspersky.es/blog/start-immunizing/19022/.
OMI (2017), "Directrices sobre la gestión de los riesgos cibernéticos marítimos", Julio, MSC-FAL.1/Circ.3.
Pérez-Salas, Gabriel (2013), "La necesaria facilitación y seguridad de los procesos logísticos en América Latina y el Caribe", *Boletín FAL* No 321, número 5, CEPAL, Naciones Unidas, Santiago.
SAFETY4SEA (2018), "Cyber attack hits Cosco's operations in US, July" [en línea] https://safety4sea.com/cyber-attack-hits-coscos-operations-in-us.
Schwab, Klaus (2020), The Fourth Industrial Revolution, World Economic Forum, ISBN-10: 1944835016, REF: 231215.
Symantec (2019), *ISTR - Internet Security Threat Report*, Volume 24, Mountain View, USA, February [en línea] https://docs.broadcom.com/doc/istr-24-2019-en.
WEF (2020), *The Global Risk Report*, 15th Edition, World Economic Forum, Switzerland.
Weikert B., Fabio (2019), "La resiliencia de los servicios de infraestructura en América Latina y el Caribe: un abordaje inicial", *Boletín FAL*, No 374, número 6, CEPAL, Naciones Unidas, Santiago.

VIII. Publicaciones de interés

Boletín FAL 381

Transformación digital en la logística de América Latina y el Caribe

Luis Valdés Figueroa
Gabriel Pérez

El presente *Boletín FAL* se inscribe dentro del tema de las reflexiones sobre tecnologías disruptivas en el transporte que la CEPAL suele realizar en estas entregas. En esta oportunidad se analiza la importancia de la transformación digital en el ámbito logístico, especialmente en el contexto actual donde la necesidad de una logística fluida, segura y resiliente demanda acciones adicionales vinculadas a la trazabilidad y a la facilitación de los procesos.

Disponible en: Español

Boletín FAL 375

La revolución industrial 4.0 y el advenimiento de una logística 4.0

Eliana Barleta
Gabriel Pérez
Ricardo Sánchez

La llamada cuarta revolución industrial (4RI) trae aparejada una serie de cambios disruptivos tanto en los modelos de negocios como en las cadenas productivas que los sustentan. La logística, como parte fundamental de estos procesos, no queda ajena a estos cambios trascendentales. Esta cuarta revolución industrial se caracteriza por la velocidad, la amplitud y profundidad en que ocurre. Los cambios son tan vertiginosos que cambiarán la manera como vivimos, trabajamos y nos relacionamos, impactando a los países, las empresas, las industrias, y la sociedad en su conjunto. El sistema logístico del futuro, en consecuencia, apunta a la interconectividad de la información, la optimización del tiempo y los recursos, con una fuerte inversión y desarrollo en innovación para mantener su competitividad.

Disponible en: Español Inglés