CAPÍTULO V

GESTIÓN DE RIESGO EN SEGURIDAD DIGITAL EN EL SECTOR PRIVADO Y MIXTO CONTEXTO GENERAL*

Arístides Baldomero Contreras

* Capítulo de libro resultado del proyecto de investigación titulado "Gestión de Riesgos en seguridad Digital" de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra, que a su vez hace parte de la línea de investigación "Seguridad Digital" del grupo de investigación "Masa Crítica", reconocido y categorizado en (B) por Colciencias. Registrado con el código COL0123247, está adscrito a la Escuela Superior de Guerra "General Rafael Reyes Prieto" de la República de Colombia.

Introducción

La popularización del uso de Internet, adicional a gran cantidad de beneficios que ha traído, ha proliferado una desmedida cantidad de riesgos en contra de las personas y las empresas, esta últimas más vulnerables día a día debido a que la mayoría de las actividades se vienen automatizando y requieren una conexión continua a Internet; síntomas vitales permiten definir y determinar que de la mano con las estrategias de negocios y para crecimiento interno del sector productivo, la seguridad digital y las políticas públicas regionales que involucren la protección por riesgos del cibercrimen o la ciberdelincuencia, sustentadas en normas claras de seguridad digital y ciberseguridad, serán aquellas que como parte integral de los planes de negocios y por supuesto del manejo de crisis y la continuidad de los mismos le permitirán salir avante en un mundo más interconectado.

La creciente transformación digital ha promovido el aumento del uso de las tecnologías de la información y las comunicaciones (TIC) en todos los aspectos de la dinámica económica y social. Esta situación también ha traído consigo nuevos riesgos asociados con la confidencialidad y protección de información, así como frente al resguardo de las infraestructuras cibernéticas que soportan los negocios explica la Asobancaria, 2018.

En el presente capítulo la preocupación inicia por el papel y la importancia del sector mixto y privado en las cifras que impactan el producto interno bruto (PIB) de cada uno de los países de la región, es un buen punto de partida para dilucidar cuáles son los productos que más

aportan o los más representativos de la economía nacional, así las cosas se debería entender que este sector en forma representativa se oferta en manera muy importante como blanco del cibercrimen y que su seguridad Digital, de la misma manera debería contar con un blindaje especial.

¿Pero es así? ¿Realmente el sector mixto privado, cuenta con las medidas necesarias de seguridad digital? O ha tomado valor ¿Cuánto viene impactando el desarrollo de la productividad en algunos de los países de Latinoamérica, o cuál es el estado de las grandes empresas como blanco de campañas delincuenciales por la vía digital?

Una reflexión en que identificamos de inmediato la preocupación de un impacto o ataque generalizado, por ejemplo en los hospitales, el sector del comercio, los restaurantes, las infraestructuras críticas, los hoteles, sin dejar a un lado, el sector financiero, integrado por las corporaciones de ahorro y vivienda (CAV), los bancos comerciales, las corporaciones financieras, los almacenes generales de depósito (AGD), las compañías de financiamiento comercial (CFC), las compañías de leasing y las sociedades de servicios financieros como las fiduciarias, los comisionistas de bolsa, las compañías de seguros, entre otras y las cuales son responsables de aportar un porcentaje cercano al 60 % del PIB.

Sin olvidar además el porcentaje adicional que proviene de otros renglones de la economía como: la explotación de minas y canteras; la electricidad, el gas y el agua; la construcción; el sector de transporte y almacenamiento; los servicios personales, los servicios del Gobierno y muchos más.

Ahora bien, de las partes y resultados ya identificados, la Política Nacional de seguridad Digital de Colombia, aprobada el pasado 11 de abril de 2016 por el Consejo Nacional de seguridad Digital, mediante la expedición del *Documento CONPES 3854* (2016), informó la necesidad de crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad Digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital.

Para ello y con el fin de alcanzar este objetivo específico, el Gobierno nacional acorde con el *CONPES 3854* (2016), debería adelantar estrategias como:

- Establecer mecanismos de participación activa y permanente de las múltiples partes interesadas en la gestión del riesgo de seguridad Digital.
- Adecuar el marco legal y regulatorio en torno a la dinámica de la economía digital y sus incertidumbres inherentes.
- Identificar y abordar los posibles impactos negativos que otras políticas pueden generar sobre las actividades de las múltiples partes interesadas o sobre la prosperidad económica y social en el entorno digital
- Generar confianza a las múltiples partes interesadas en el uso del entorno digital.
- Promover comportamientos responsables en el entorno digital en diferentes niveles de formación educativa.

Aspecto que se abordará en particular más adelante y para entender el estado actual y a manera de insumo con el fin de seguir generando instrumentos pertinentes con relación al cumplimiento de la política definida y la priorización del desarrollo de los planes futuros en la materia; resulta conveniente y de gran interés que se identifiquen cuáles son los principales incidentes, amenazas y ataques contra la seguridad digital (tratados como los que se producen a la seguridad cibernética y/o seguridad de la información) que están afectando a los países, reconocer sus principales blancos u objetivos y conocer los costos económicos que estos representan para el sector mixto – privado.

Cabe aquí recordar la Declaración sobre Seguridad en las Américas (2003) aprobada por el Consejo Permanente en su reunión ordinaria, celebrada el día 22 de octubre de 2003 y en la cual firmemente convencidos de que, en vista de los cambios profundos que han ocurrido en el mundo y en las Américas desde 1945, se tenía una oportunidad única para reafirmar los principios, valores compartidos y enfoques comunes sobre los cuales se basa la paz y la seguridad en el hemisferio. Declaró entre sus valores compartidos y enfoques comunes, en su literal e) lo siguiente:

> En nuestro Hemisferio y en nuestra condición de Estados democráticos comprometidos con los principios de la Carta de las Naciones Unidas y la

> Carta de la OEA, se reafirmaba que el fundamento y razón de ser de la seguridad es la protección de la persona humana y que la seguridad se fortalecía cuando profundizamos en su dimensión humana, pero también se expresó que las condiciones de la seguridad humana mejorarían mediante la promoción del desarrollo económico y social, del cual como hemos leído en cifras anteriores son responsables las organizaciones del sector mixto – privado, las cuales aportan un porcentaje cercano al 60 % del PIB.

Además la Declaración sobre seguridad en las Américas (2003) explicó que las amenazas, preocupaciones y otros desafíos a la seguridad en el hemisferio son de naturaleza diversa y alcance multidimensional y el concepto y los enfoques tradicionales deben ampliarse para abarcar amenazas nuevas y no tradicionales, que incluyen aspectos políticos, económicos, sociales, de salud y ambientales, sumando por lo tanto que se debían incluir decisivamente los ataques a la seguridad cibernética.

1. Situación actual

Por su parte, tomando como ejemplo y en forma inicial, el estado de la seguridad digital de Colombia, en el año 2017 se determinó el nuevo blanco de los cibercriminales, claramente enfocado en las empresas, sector productivo de la economía; con el cambio en la selección de las víctimas, pasando del ciudadano común a las grandes empresas del sector público y privado, las cuales generan una mayor rentabilidad a la actividad criminal, explicó el Centro Cibernético Policial (2017).

Nótese que el estudio realizado por la Organización de los Estados Americanos, MINTIC y BID (2017) denominado Impacto de los incidentes de seguridad digital en Colombia, iniciativa pionera en la región y poco frecuente a nivel mundial, representa un factor importante en la medida en que revela información sobre las amenazas para la seguridad digital en un país y analiza la capacidad del mismo para defenderse ante dichas amenazas, lo cual es difícil de recolectar.

El mismo informe sitúa al gobierno de Colombia en la vanguardia de la generación de conocimiento en el área de la seguridad digital, que

facilita el diseño y la implementación de políticas y que atiendan a los aspectos más débiles de escenarios reconocidos.

Sin embargo, el informe muestra que al preguntar a las organizaciones colombianas, si creen que están preparadas para hacer frente a un incidente digital, un promedio simple del **37%** de las empresas que participaron del estudio (empresas de los sectores Servicios, Industria y Comercio) explicaron que estaban preparadas para manejar un incidente digital, dejando por fuera el **63 %** que es un cifra preocupante.

De llamar la atención, entre las medidas más importantes que se pudieron identificar para asegurar las organizaciones colombianas frente a los incidentes digitales, es la identificación de un cargo con dedicación exclusiva para el manejo de este tipo de incidentes, este cargo es importante ya que les ayudará a las entidades a detectar, aislar y resolver incidentes rápidamente cuando ocurran, explicó la Organización de los Estados Americanos *et al.* (2017)

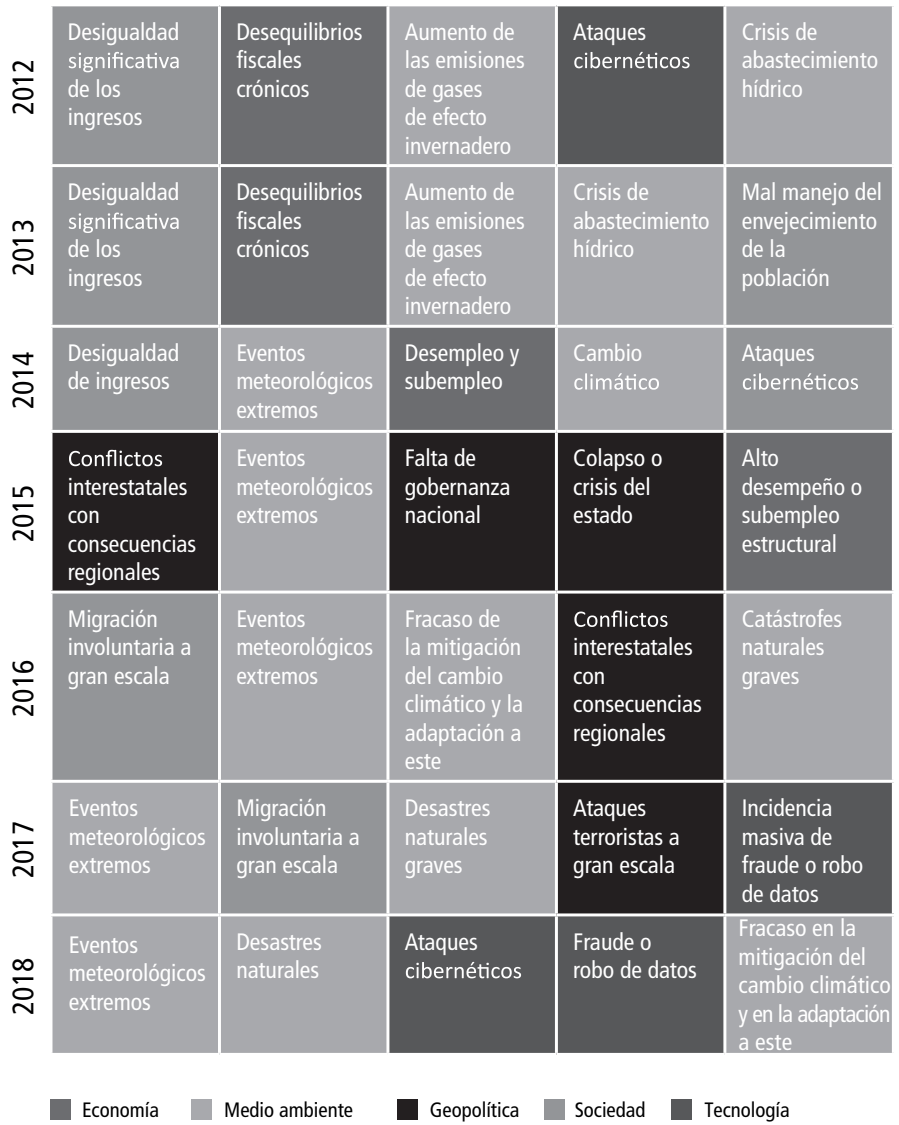
Por otro lado, y para no dejar descartar y llamar la atención a la importancia del estado actual de los riesgos para la ciberseguridad, explica el Foro Económico Mundial (2018) que estos riesgos también están aumentando tanto en su prevalencia como en su potencial desestabilizador. Los ataques contra las compañías casi se ha duplicado en cinco años y los incidentes que antes se consideraban extraordinarios son cada vez más comunes.

El impacto financiero producto de las violaciones de seguridad cibernética está aumentando y algunos de los mayores costos de 2017 están relacionados con los ataques mediante programas de secuestro cibernético, que representaron el 64 % de todos los correos electrónicos maliciosos.

Algunos ejemplos notables incluyeron el ataque WannaCry, que afectó a 300.000 computadoras en 150 países, y NotPetya, que causó pérdidas trimestrales de USD 300 000 000 a varias compañías afectadas.

Otra tendencia creciente es el uso de ataques cibernéticos dirigidos a la infraestructura fundamental y los sectores industriales estratégicos, lo que nos lleva a temer que, en el peor de los casos, los atacantes podrían desencadenar un colapso de los sistemas que mantienen a las sociedades en funcionamiento.

Figura 1. Los cinco riesgos globales en términos de probabilidad por el Foro Económico Mundial (2018)



Fuente: Panoramas de riesgos en evolución, 2008–2018. Informe de riesgos mundiales 2018, 13.a edición. Ginebra p. 6.

1.1. Estado y panorama de Latinoamérica en países acorde con políticas y estrategias nacionales de seguridad digital y cibernética

Frente a la seguridad digital, América Latina y Caribe requieren mayores esfuerzos en ciberseguridad, esto toda vez que la región presenta vulnerabilidades "potencialmente devastadoras" y donde cuatro de cada cinco países carecen de estrategia de ciberseguridad, resaltó el BID y OEA (2016).

Entonces, es menester mencionar algunos casos sobre el estado de adhesión en políticas de seguridad digital para la región.

Colombia 2011 – 2016

El Consejo Nacional de Política Económica y Social del Gobierno de Colombia estableció la Política nacional de seguridad cibernética *CONPES 3701* bajo el auspicio del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), el Ministerio de Defensa, el Departamento Nacional de Planeación y otras instituciones nacionales clave.

Además, en 2014 una Misión de Asistencia Técnica de la OEA ayudó al país a construir la capacidad con las partes interesadas para desarrollar marcos y políticas institucionales.

El Grupo de Respuesta de Emergencias Cibernéticas de Colombia (ColCERT) es una institución clave en defensa y seguridad cibernética y se muestra competente para la coordinación con otros organismos y el sector privado. En Colombia funciona un mecanismo de respuesta a incidentes cibernéticos específicos y los programas de gestión del riesgo han comenzado a surtir efecto.

Colombia cuenta, como bien se mencionó, con Política Nacional de Seguridad Digital, aprobada en abril de 2016 al expedirse el Documento *CONPES 3854 (2016).*

Por otro lado, Colombia que fue el primer país de la región en tomar muy en serio este tema, ha captado la atención mundial, pero aunque esta información podría ser curiosa no lo es, debido a que Colombia se

encontraba inmersa en una lucha interna contra las Fuerzas Armadas Revolucionarias de Colombia (FARC) durante varias décadas, una lucha que hace que las Fuerzas Militares y la Policía, en coordinación con el sector privado, defiendan y protegieran la Infraestructura Critica, física y virtual del país.

Por tanto, en la etapa final de su política nacional de ciberseguridad y ciberdefensa (CONPES 3701/2011), se formaron grupos de trabajo y se incluyeron a las instituciones del Gobierno nacional (Ministerio de Defensa Nacional, MinTIC, la Policía Nacional, etc.) y a las organizaciones del sector privado (representantes de los sectores de energía y comunicaciones, administradores de los dominios.co, universidades, etc.) con los cuales se creó un marco serio y coordinado que buscó proteger las infraestructuras críticas del país, denominado según el documento *CONPES 3854/2016* y desde el pasado 11 de abril de 2016 "la Política Nacional de Seguridad Digital".

En primer lugar, se estableció un marco institucional claro en torno a la seguridad digital. Para esto, se crearon las máximas instancias de coordinación y orientación superior en torno a la seguridad digital en el gobierno, y se establecieron figuras de enlace sectorial en todas las entidades de la rama ejecutiva a nivel nacional.

En segundo lugar, se crearon las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital, mediante mecanismos de participación activa y permanente, la adecuación del marco legal y regulatorio de la materia y la capacitación para comportamientos responsables en el entorno digital.

Como tercera medida, se fortaleció la defensa y seguridad nacional en el entorno digital, a nivel nacional y trasnacional, con un enfoque de gestión de riesgos y por último, se siguen generando mecanismos permanentes para impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional, con un enfoque estratégico.

Para poner en marcha esta política, se ha construido un plan de acción que se está ejecutando desde el año 2016 a 2019 con una inversión total de 85.070 millones de pesos. Las principales entidades ejecutoras

de esta política son el Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Defensa Nacional, la Dirección Nacional de Inteligencia y el Departamento Nacional de Planeación.

Se estima que la implementación de la política nacional de seguridad digital al año 2020 podría impactar positivamente la economía de Colombia, generándose durante los años 2016 a 2020 alrededor de 307 000 empleos y un crecimiento aproximado de 0.1% en la tasa promedio de variación anual del Producto Interno Bruto (PIB), sin generar presiones inflacionarias.

Brasil 2014

El país más grande de América Latina también es el más digitalizado y ha hecho la mayor inversión en TI de la región. Adicionalmente, es el cuarto país con el mayor número de usuarios de Internet del mundo con más de 100 millones de personas conectadas a Internet, gracias a los incentivos del gobierno. La presidencia de la República aprobó el Marco Civil de Internet en abril de 2014, el cual plantea las reglas, los derechos y las obligaciones del uso de Internet, así como la protección de los datos.

Panamá 2013

Desde mayo de 2013, el Gobierno de Panamá ha estado trabajando en la implementación de su Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructura Crítica (ENSC+IC), desarrollada por la Autoridad Nacional para la Innovación Gubernamental (AIG). Este documento, junto con un informe de posición titulado "La Resiliencia de la Infraestructura Crítica, Protección de Menores en Internet y Seguridad Cibernética", establece metas y diseña papeles y responsabilidades. Desde entonces, las entidades del gobierno han comenzado las etapas iniciales del desarrollo de planes internos de seguridad cibernética.

Trinidad y Tobago 2013

En respuesta a una serie de ataques cibernéticos en 2011, el Marco de Políticas de Mediano Plazo de Trinidad y Tobago reconoció

oficialmente tanto el papel que desempeñan las TIC en la promoción del desarrollo y el crecimiento económico nacional como la necesidad de implementar iniciativas efectivas de seguridad cibernética para proteger esta infraestructura central. En diciembre de 2012 el Ministerio de seguridad Nacional publicó una Estrategia Integral Nacional que detalla los riesgos cibernéticos del país y establece las funciones y responsabilidades de las entidades.

Jamaica 2015

En 2013 el Gobierno de Jamaica no tenía en marcha políticas ni estrategias de seguridad cibernética. Dos años después, ya ha diseñado una Estrategia Nacional Integral, presentada el 28 de enero de 2015. Cuenta con un Grupo Nacional de Trabajo de seguridad Cibernética, establecido bajo el Ministerio de Ciencia, Tecnología, Energía y Minería. El Programa de Seguridad Cibernética de la OEA y otras organizaciones internacionales han ayudado a Jamaica en el desarrollo de su CSIRT. Cabe destacar que a raíz de una serie de ataques cibernéticos contra sitios web del gobierno a finales de 2014, la OEA envió un equipo de expertos a Kingston para dar apoyo en la gestión de incidentes.

Los nuevos países que se han adherido a la formulación de políticas públicas en materia de seguridad Digital en el 2017 son: Costa Rica, Paraguay, Chile, México, República Dominicana.

Guatemala 2018

Pero estas se fundamentan y avanza según los pilares jurídicos de los países partes de la región, algunos de ellos han sumado a sus ordenamientos penales contemplar los delitos informáticos, la mayoría de los países en Latinoamérica, luego de la invitación han firmado su adhesión al Convenio sobre la Ciberdelincuencia o Convenio de Budapest.

> "Convencidos de la necesidad de aplicar, con carácter prioritario, una política penal común con objeto de proteger a la sociedad frente a la ciberdelincuencia, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional" (Convenio de Budapest, 2001).

Además, que el Convenio reconoce la cooperación entre el sector privado y los gobiernos, en aras de la necesidad de protección de "los intereses legítimos en la utilización y el desarrollo de las tecnologías de la información; estimando que la lucha efectiva contra la ciberdelincuencia requiere de una cooperación internacional reforzada, rápida y eficaz en materia penal".

En Latinoamérica los países firmantes son:

Tabla 2. Países firmantes

PAÍS	FECHAS
Argentina	5 de junio de 2018
Colombia	(En Proceso Interno)
Costa Rica	22 de septiembre de 2017
República Dominicana	17 de febrero de 2013
Panamá	5 de marzo de 2014
Paraguay	(En Proceso Interno)
Perú	(En Proceso Interno)

Fuente: Council of Europe (23 de julio de 2018). Sitio oficial COE

Indica Miró (2012) que, para llegar a comprender el cibercrimen, para prevenirlo, es muy importante entender la forma en que las personas interactúan con el ciberespacio cada día e incluso a cada hora, dónde lo hacen y el modo en que trabajan. Resalta que se debe pensar asimismo en la relación que guarda el uso del ciberespacio con los extensos patrones de la vida diaria.

Suma a sus comentarios que cualquier persona que trabaje de noche podría: "hacerse con contraseñas o utilizar los ordenadores de empresas que no estén bajo vigilancia, un padre que no supervise a su hijo adolescente durante el día o durante el viaje de fin de semana podría desconocer que se ha iniciado en el cibercrimen o que es víctima de este".

Señala Cohen y Felson (1979) que el crimen se produce durante los actos cotidianos del día a día, cuando se unen en el espacio y el tiempo un objetivo adecuado, un delincuente motivado y sin un guardián capaz de darle protección al primero.

Pues bien, como se ha señalado en las páginas anteriores el sector mixto – privado es de gran interés para los gestores de la criminalidad digital, solo al revelar que más del 63 % de las organizaciones del sector mixto – privado explicaron que no estaban preparadas para manejar un incidente digital, lo que constituye una desventaja y si se tiene en cuenta que este tipo de organizaciones se encuentre en un país con falta de políticas se seguridad, se complementa como un espacio perfecto para la comisión del mismo.

Queda claro que al analizar en qué medida el ciberespacio se configura como un nuevo ámbito de oportunidad criminal, obliga a repensar las estrategias de prevención de la delincuencia y de qué forma podemos adaptar las enseñanzas de la Teoría de las Actividades Cotidianas también tratada por Cohen y Felson (1979).

La seguridad misma del gremio es un reto, ya sea por su importancia en la economía o por el papel que juega en el PIB de cada país, sumado a la aceleración y el grupo de motivos que nos llevan a cumplir los principios de la nueva revolución industrial y a la transformación digital para la prestación de los servicios.

A la fecha la criminalidad digital sigue incrementándose, debo mencionar que esto obedece también a la falta de compromiso en la denuncia, hay suficientes razones para que el cibercrimen sea particularmente difícil de cuantificar y cuando obedece en las empresas la necesidad de proteger la reputación se cierra la oportunidad de la no repetición en el sector al cual pertenezca la organización afectada.

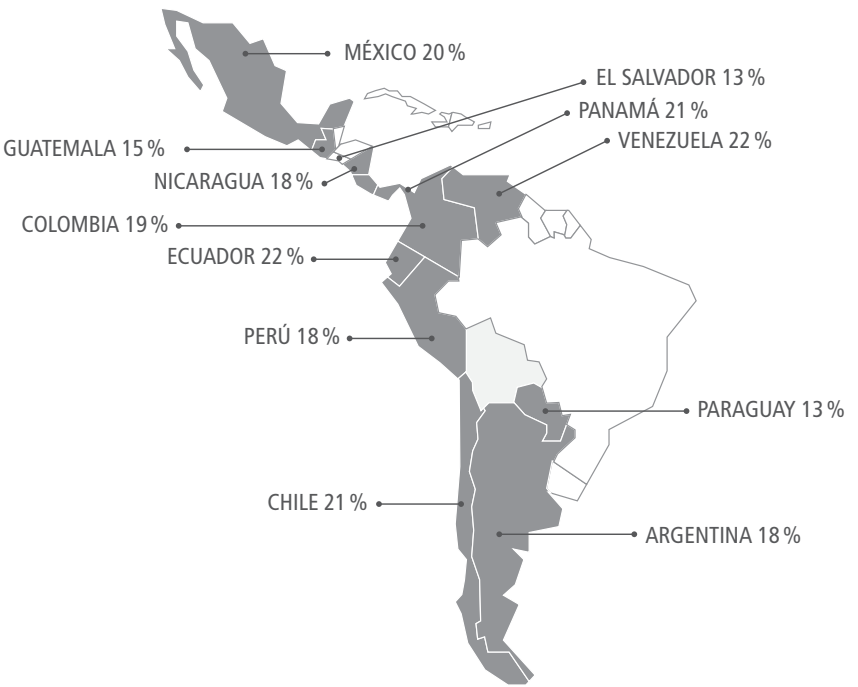
Debemos aunar esfuerzos y mantener un enfoque actualizado, en equipo y de transferencia de información, sucede a menudo que la víctima (persona u organización) no se da cuenta del ataque al que fue expuesto, o cuando ya lo hace lo entiende demasiado tarde para poner en conocimiento, estos comportamientos llevan en general a un apoyo indirecto de la criminalidad digital.

1.2. El inminente crecimiento de las infecciones y ataques a la seguridad digital en la región

A medida que pasa el tiempo, cifras evidentes resultan la importancia de la seguridad digital, al menos tres de cada cinco empresas en la región sufrieron por lo menos un incidente de seguridad, estando en el top la infección con códigos maliciosos (45 %). La mitad de ellos aparecen relacionados al *ransomware*, es decir que al menos una de cada cinco empresas encuestadas en toda Latinoamérica fueron víctimas del secuestro de información, explica ESET Latinoamérica (2018).

La figura 2 identifica el porcentaje de infecciones; no existe una gran diferencia entre las empresas de cada país, siendo Ecuador el que tiene un mayor índice de infecciones de *ransomware* y El Salvador el que tiene el menor.

Figura 2. Porcentaje de infecciones de *malware* por país



Fuente: ESET Security Report Latinoamérica 2018

De la misma manera, Kaspersky Lab registró más de 746 mil ataques de *malware* diarios durante los últimos 12 meses en América Latina, lo que significa un promedio de 9 ataques de malware por segundo. Además, los ataques de *phishing* – correos engañosos para el robo de la información personal de los usuarios– han sido constantes en la región, principalmente en Brasil.

Los resultados, presentados durante la Octava Cumbre de Analistas de seguridad para América Latina que se está realizando en la ciudad de Panamá, demuestran que toda la región ha experimentado una considerable cantidad de ciberamenazas, con la gran mayoría orientada al robo de dinero.

Hubo un incremento del 60% en ataques cibernéticos en la región, donde Venezuela registra el mayor número de los ataques en proporción a su población con un total de 70.4%, seguido por Bolivia (66.3%) y Brasil (64.4%). Al igual que en 2017, Brasil continúa encabezando a los países latinoamericanos en términos de alojamiento de sitios maliciosos ya que 50% de los hosts ubicados en América Latina que se utilizaron en ataques a usuarios de todo el mundo está ubicado en este país.

Según los datos de la empresa, la mayoría de estos ataques ocurre en línea, mientras se está navegando, descargando archivos o cuando reciben adjuntos de correos electrónicos engañosos y afectan más a los usuarios domésticos que a empresas. Sin embargo, la investigación también reveló que las empresas son más propensas a ataques vía email (60 %) y vectores *offline* (43%); es decir, través de USB contaminadas, la piratería de *software* u otros medios que no requieren el uso obligatorio del Internet.

El año 2017, Brasil también estuvo dentro de los 20 países más atacados a nivel mundial. Esto se debe, en gran parte, a que los cibercriminales utilizan el correo electrónico, mensajes de SMS, llamadas telefónicas, anuncios en redes sociales, entre otros, con nombres de empresas conocidas, lo que hace que los usuarios no desconfíen de esos mensajes, aumentando la probabilidad de que estos sean compartidos con su red de amigos (Assolini, 2018).

Y es que ya el aumento de los ataques cibernéticos en América Latina se había alertado que fue de un 59 % entre 2016 y 2017. Además, explica que cada vez son más diversos, sofisticados, potentes y con mayor alcance e impacto, así lo deja saber también en Colombia, el informe del Centro Cibernético Policial (2017), en el cual el cibercrimen del país aumentó un 28.3 %.

Aunque en Colombia, el Estado ha avanzado en la definición de una Política Publica de ciberseguridad y en el fortalecimiento institucional, debido a los enormes impactos que podría tener un incidente en la seguridad Digital de las organizaciones, no solo en términos netamente monetarios sino en perdida de información y amenaza sobre la reputación, todas las instituciones públicas y privadas deben trabajar en el fortalecimiento de sus capacidades para anticiparse a las ciberamenazas.

Resalta la Asociación Bancaria y de Entidades Financieras de Colombia, Asobancaria (2018) en cuanto a los esfuerzos por la articulación de políticas públicas para la protección ante los ciberataques o actividades que expongan nuestra seguridad Digital: "Es previsible que la expedición de esta regulación acelere los avances en la constitución de un Sistema de Gestión de Riesgos de Ciberseguridad e implique reorganizaciones al interior de cada institución para fortalecer sus capacidades frente a las amenazas cibernéticas".

El sector privado y mixto como motor de la economía, mientras en la mayoría de los delitos tradicionales y para obtener una buena rentabilidad se hacía necesario un mayor esfuerzo superior, en los delitos informáticos de la nueva era, el esfuerzo es mínimo y la recompensa siempre es alta, Centro Cibernético Policial (2017).

Por ello las dinámicas del cibercrimen y su constante evolución exponencial, han propiciado que delincuentes que hasta hace poco actuaban de manera aislada, sin coordinación y con un alcance local, constituyan en la actualidad organizaciones trasnacionales complejas de cibercrimen.

Panoramas internacionales como el de Estados Unidos de América nos ayudan a dimensionar el alcance del acceso a la Internet y del ciberespacio, reconocido en forma asertiva y preocupante como una potencial sorpresa al evaluar las amenazas de la seguridad nacional de los

próximos años, y que seguirán en aumento y más allá todavía de lo imaginado, ya que miles de millones de dispositivos digitales nuevos estarán conectados, con relativamente poca seguridad incorporada, y tanto los estados nacionales como los actores malignos se volverán más valientes y mejor equipados en el uso de herramientas cibernéticas que cada vez están más extendidas (Coats, 2018).

Por ende, el compromiso a dimensionar en el sector mixto y privado, se debe conectar con las necesidades y las nuevas prestaciones de las nuevas tecnologías, evaluando y motivando sobre las preocupaciones en los nuevos riesgos, so pena de encontrarse como organizaciones donde no se cuenta con procesos de seguridad, o donde no se plasman dentro de sus panoramas de riesgos las nuevas estratégicas o *Modus operandi* delincuencial, la evaluación asociada al cibercrimen, el ciberterrorismo, ciberactivismo o el ciberespionaje, es entendible que requerirá mayor acción y participación desde la sociedad y más aún desde el sector productivo.

2. Sector en el futuro

Tal y como lo explica el Centro Cibernético Policial (2017), la lógica de que esta "novedad" dure tanto, es la revolución de las TIC, como concepto amplio, abierto y dinámico que engloba todos los elementos y sistemas utilizados en la actualidad para el tratamiento de la información, su intercambio y comunicación en la sociedad actual, se enmarca bajo el fenómeno del cibercrimen que no ha terminado todavía, ni lo hará en mucho tiempo, lo que supone que la cibercriminalidad o delincuencia asociada al ciberespacio y la seguridad Digital seguirá evolucionando en las próximas décadas.

2.1. Retos frente a los delitos informáticos en el sector mixto – privado

La red informática se caracteriza por prestar un servicio de comunicación que no reconoce fronteras, día tras día los negocios y en especial la relación de oportunidades corporativas trasciende a escenarios digita-

les para lograr objetivos estratégicos ante la competencia.

La digitalización es ahora una mega tendencia, pero ¿dónde queda la seguridad Digital de esta? Hay millones de dispositivos conectados a Internet que permiten hacer las cosas de forma muy distinta y fácil, más clientes necesitados de servicios y productos. Toda vez que el llamado a las empresas es emprender esta revolución y observando que lo que se requiere es aporte de conocimiento para que sean más globales y eficientes, surgen grandes interrogantes.

¿Están realmente las organizaciones capacitándose e implementado actividades bajo las nuevas tendencias y retos de la seguridad digital?

Este es el primer reto que deben evaluar las Empresas, si la respuesta es afirmativa en ese caso, se suma a un nuevo desafío ¿Están preparadas las empresas del sector mixto – privado, en la implementación de plataformas que brinden seguridad de sus servicios para lograrlo?

Descrito en la Comunicación oficial de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones, la cual resalto la necesidad de creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos (Comisión de las comunidades europeas, 2000).

> Las infraestructuras de información y comunicación se han convertido en una parte crucial de nuestras economías. Desafortunadamente, estas infraestructuras tienen sus propias vulnerabilidades y ofrecen nuevas oportunidades para la delincuencia. Estas actividades delictivas pueden adoptar una gran variedad de formas y pueden cruzar muchas fronteras. Aunque, por diversas razones, no existen estadísticas fiables, no cabe duda de que estos delitos constituyen una amenaza para la inversión y los activos del sector, así como para la seguridad y la confianza en la sociedad de la información. Ejemplos recientes de denegación de servicio y ataques de virus han causado grandes perjuicios financieros, puede actuarse tanto en términos de prevención de la actividad delictiva, aumentando la seguridad de las infraestructuras de información, como garantizando que las autoridades responsables de la aplicación de ley cuenten con los medios adecuados para intervenir, respetando plenamente los derechos fundamentales de los individuos (Comisión de las comunidades europeas, 2000).

Ello supone, que toda prestación de servicios digitales deberá ofrecer soluciones ante uno de los retos principales, denominado "Confianza del cliente o del usuario digital" paradigma de prevención que enfrenta la nueva clase de delitos digitales y/o tecnológicos, bajo el alcance de las normas internacionales en la materia y las políticas públicas de cada país.

Casos que al analizar permiten vislumbrar en forma precisa, cuáles son los retos puntuales que la regulación colombiana y la Jurisprudencia en la materia posicionan hacia el sector.

Estos retos, sin el ánimo de cerrar la brecha a más posibilidades, pueden detallarse así:

1. Seguridad de los servicios que ofrece y de las operaciones que permite realizar en relación con las plataformas digitales.

2. Seguridad como uno de los deberes significativos en la relación empresa – cliente. La obligación de seguridad puede considerarse como aquella en virtud de la cual una de las partes del contrato se compromete a devolver al otro contratante, ya sea en su persona o en sus bienes, sanos y salvos a la expiración del contrato, pudiendo ser asumida tal obligación en forma expresa por las partes, ser impuesta por la ley, o bien surgir tácitamente del contenido del contrato a través de su integración sobre la base del principio de buena fe.

3. Reconocimiento de partes débiles a los clientes en toda relación de consumo, y por ende que el ordenamiento jurídico promueva su protección y exija a las entidades un proceder consonante con el interés colectivo trascendente de protección al consumidor que emana de lo estatuido por los *Artículos 78* y *335* de la Constitución Política, lo que justifica la serie de obligaciones, cargas y conductas exigibles a dicho profesional, amén de un régimen de responsabilidad diferente del común.

4. Necesidad de entendimiento de la Teoría del riesgo creado. "La teoría del riesgo, impregnada por el valor moral de la solidaridad, parece sobre todo inspirada por la equidad: Por su actividad, el hombre puede

procurarse un beneficio (o, al menos, un placer). Es justo (equitativo) que en contrapartida él repare los daños que ella provoca. Ubi emolumentum, ibi onus (ahí donde está la ventaja, debe estar la carga) (Díez L., 1999).

Su fundamento, según el autor precitado, resulta "del poder que tenía el responsable de evitar el daño. O para decirlo de otra manera por vía de una expresión a la cual nosotros adherimos y que empleamos usualmente, en su dominio; dominio que él tenía o, al menos, habría debido normalmente tener, de su actividad, así como de los hombres o de las cosas por las que él responde" (Trigo, y López, 2004).

Para lo cual, en su aplicación a las actividades del sector mixto o privado, se debe sostener que la relación existente entre el cliente y la empresa, requiere un intercambio continuo de confianza, a tiempo en que también determina la reciprocidad de esfuerzos en la tarea de evitar posibles daños por descuido o incumplimiento de las obligaciones contractuales de las partes, que con ello tendrá por entendidas también, las que le impongan como cargas por la ley a través de la presunción de responsabilidad.

5. Las nuevas tecnologías y el riesgo de la actividad empresarial en medios digitales. Afianzado bajo el concepto y la premisa de la modernización de la distribución de productos y servicios, lo que determinó el paso de las oficinas físicas a la atención al cliente por otros canales transaccionales como los cajeros electrónicos, los sistemas de audio respuesta, los centros de atención telefónica o *call center*, los sistemas de acceso remoto para clientes (RAS), el Internet y, recientemente, las aplicaciones en dispositivos móviles.

Estas últimas que en efecto requieren de rigurosos esquemas de seguridad y protección de la información que por ellos circula, pues a través de estas se realiza la disposición de los recursos monetarios de los clientes.

En ese sentido, se ha dicho que la "difusión de la informática en todos los ámbitos de la vida social ha determinado que se le utilice como instrumento para la comisión de actividades que lesionan intereses jurídicos y entrañan el consiguiente peligro social…"

6. Mayores exigencias, cargas y deberes según la actividad a desarrollar en el ambiente digital. Como lo ha explicado la Corte Suprema de Justicia, Sala de Casación Civil de la República de Colombia, al decidir recurso de reposición el pasado diecinueve (19) de diciembre de dos mil dieciséis (2016) SC18614-2016 Radicación No 05001-31-03-001-2008-00312-01 Magistrado Ponente Ariel Salazar Ramírez.

> "El riesgo, entonces, se materializa con el ofrecimiento a los clientes de una plataforma tecnológica para realizar sus transacciones en línea, la cual puede ser vulnerada por delincuentes cibernéticos a través de diversas acciones, atendida la vulnerabilidad inherente a los sistemas electrónicos".

No obstante, el uso de éste lleva ínsito el riesgo de fraude electrónico, el cual es de la institución financiera precisamente por la función cumplida por las instituciones financieras y el interés general que existe en su ejercicio y la confianza depositada en él, lo que determina una serie de mayores exigencias, cargas y deberes que dichas entidades deben cumplir con todo el rigor; por el provecho que obtiene de las operaciones que realiza; por ser la dueña de la actividad, la que **se reitera** tiene las características de ser profesional, habitual y lucrativa; y además, por ser quien la controla, o al menos, a quien le son los exigibles los deberes de control, seguridad y diligencia en sus actividades, entre ellas la de custodiar dineros provenientes del ahorro privado.

Por eso, por una parte las instituciones financieras están compelidas a adoptar mecanismos de protección de los datos transferidos en relación con sus usuarios, a través de los cuales pueda prevenirse la defraudación, pues para el momento en que estos son detectados, generalmente, ya se ha causado el daño patrimonial, y por otra, están sujetas a la responsabilidad que acarrea para ellas la creación de un riesgo de fraude que afecta a sus clientes, a disposición de los cuales ha dispuesto su plataforma y recursos tecnológicos.

2.2. Seguridad y mantener la confianza en el sector mixto – privado

Sumado a lo anterior, la **"Seguridad y Mantener la Confianza"** y que esta se apropie y se mantenga alineada con el impacto de los ciberataques, trae un cuestionamiento muy importante a realizar.

¿Cómo contar la seguridad digital necesaria, como proteger nuestros activos claves y las operaciones? Reto para identificar las nuevas amenazas y a las que se está expuesto, la evaluación y pruebas para saber que proteger, sumado a la resiliencia digital y cibernética para saber dónde se es vulnerable.

Reconocer la necesidad de contar con enfoques más alineados en lo que más le importa a cada negocio y al impacto de los ciberataques, el sector mixto – privado por su carácter de importancia en la cadena de valor e impacto en (PIB) Producto Interno Bruto de los países, obliga a realizar enfoques basados en riesgos, direccionar estrategias cibernéticas e inversión, acorde a las capacidades cibernéticas detectadas y que proporcionen la mejor protección a los activos claves y las operaciones previamente establecidos.

Con los datos y la transformación digital ahora en el corazón de las operaciones y las nuevas oportunidades que conlleva la apertura del mundo con la virtualización; la seguridad digital y cibernética deberá gestionarse, dotarse de recursos e integrarse adecuadamente, para "mantener la confianza" y permitir el éxito.

El uso de los datos significa conectarse con un mundo más interconectado, la seguridad digital es necesaria, deja en claro como estamos reduciendo el riesgo y permite un cambio radical en los recursos y los controles, prioriza estos para reducir pérdidas y establece una Estrategia Cibernética Personalizada.

"No debe perderse de vista que el paradigma sobre el que descansan la nueva generación de delitos informáticos" o con ausencia de seguridad digital, "Se halla en el valor estratégico asignado a la información (los datos), y la respectiva protección de los sistemas de transmisión de dichos datos". Así mismo, "La seguridad no se trata solamente de una

solución tecnológica, ya que también hay un componente humano que es necesario proteger".

El primer paso o característica de las grandes empresas o de las representaciones de organizaciones transnacionales, cuando se realiza un proceso laboral o de inducción a un nuevo empleado, es la entrega de un artículo electrónico digital conectado a la Internet.

ESET Latinoamérica menciona que de acuerdo con encuestas realizadas en Latinoamérica por parte de su organización.

> Solamente el 30 % de los usuarios utiliza una solución de seguridad en sus dispositivos móviles, a pesar de que más del 80% reconoce que los usuarios son los que tienen la mayor cuota de responsabilidad al momento de caer en engaños por no tomar consciencia ni educarse sobre las diferentes estafas. (ESET, 2018)

Ello trae una importante consideración a tener en cuenta en el continente, la cibercriminalidad y los retos de su prevención van ligados directamente a las diferentes medidas que sean establecidas para que la decisión de actuar del cibercriminal, este valora el esfuerzo necesario que va a tener que realizar para cometer el delito, este agresor potencial ya reconoce que las pequeñas y mediana empresas son blancos importantes y llenos de información vital con grandes utilidades y menor seguridad.

En resultados obtenidos de investigaciones y encuestas, se reveló que hay una consolidación de la función de gestión de ciberriesgos y seguridad de la información, los ejecutivos responsables de administrar la seguridad de la información consideran que aún no cuentan con recursos suficientes y son conscientes que tienen un largo camino por recorrer.

Entre los mayores desafíos a conocer por parte de las organizaciones y en particular las del sector mixto – privado en Latinoamérica, se destacan en la implementación de capacidades de monitoreo de riesgos y de respuesta ante incidentes y brechas de seguridad de la información. "Esto resulta de relevancia considerando que 4 de cada 10 organizaciones han sufrido una brecha de seguridad en los últimos 24 meses" (Deloitte, 2016).

El camino para que las empresas del sector mixto y privado se conviertan en organizaciones adaptadas a los riesgos de seguridad Digital, debe iniciarse a partir de la toma de conciencia y en los altos niveles directivos y ejecutivos de la organización, reconocer las ciberamenazas propias del nuevo ambiente digital de negocios, hablar e incluir en los presupuestos organizacionales cifras importantes para atender lo que, a la fecha, ya es un flagelo que genera grandes pérdidas. Comprender el nivel de exposición y qué se puede hacer para mejorar, es el primer paso que los Ejecutivos y encargados de gestionar los riesgos digitales deben dar.

Uno de los elementos que pueden conformar el perfil y la oportunidad delictiva del cibercriminal va asociado al ámbito de oportunidad y a la perspectiva preventiva adoptada; justamente y en desarrollo de la presente investigación, en el año 2018 los países de Guatemala y República Dominicana presentaron sus estrategias nacionales de ciberseguridad, sumado a ello ya son 10 países de la Región que han adoptado procesos para protegerse en el ciberespacio, un esfuerzo conjunto de gobierno, sector privado y sociedad civil, y con amplia participación y apoyo del Programa de ciberseguridad que ahora trabaja con todos los países de la Organización de Estados Americanos (OEA).

La velocidad con la que aparecen las nuevas tecnologías, los nuevos reportes de ataques, las familias de *malware* o las fallas de seguridad con impacto global, hacen de la seguridad un desafío cada vez más importante para las empresas, los gobiernos y los usuarios alrededor del mundo, si bien es cierto en la actualidad se invita a las pequeñas, medianas y grandes empresas a explorar nuevos espacios y a descubrir ideas innovadoras sobre los productos o servicios que cada empresa ofrece, se les invita a la innovación, a nuevos formatos de planeación estratégica para lograr mejores resultados, ¿Dónde y cómo se habla de la seguridad para estos procesos?

Es importante reconocer cada uno de los interrogantes que se plantean en cada espacio de reflexión, los cuales se enmarcan en la medida de evaluación "Digitalización Vs Migración Segura, ¿es oportuna y consecuente en forma apresurada?"

Conclusiones

Supervivencia organizacional bajo una gestión oportuna de seguridad digital

Son muchos los retos que quedan en la consolidación de la seguridad digita; la privacidad y los secretos empresariales; el sector mixto privado debe proteger sus ventajas competitivas, conocer y reconocer las amenazas cibernéticas que más se presentaron en los países de la región; reconocer los tópicos de la consolidación del *Crime as a Service*, el cual, como riesgo y amenaza se fundamenta en la modalidad donde se disponen servicios, generalmente a través de la web, para que cualquier persona sin conocimientos profundos en tecnología los pueda contratar.

Al hablar de controles de seguridad, probablemente sean muchos los que piensen en contar con alguna solución de seguridad o tecnología de protección, pero pocos se plantearán la opción de incluir políticas y planes para gestionar la seguridad de la información. Y toda vez que esto último se ve reflejado en empresas de Latinoamérica, la tecnología no lo es todo a la hora de hablar de seguridad, sino que deberá complementarse con una adecuada gestión, concientización y capacitación; y es en este punto donde se encuentran las mayores diferencias y los principales riesgos.

Quizás uno de los puntos más débiles en cuanto a seguridad digital son las tecnologías de seguridad relacionadas con los dispositivos móviles pues, en su mayoría, este tipo de equipos no cuentan con soluciones de seguridad efectivas.

Otro punto que también resulta preocupante y que cabe destacar, es la baja adopción de tecnologías, como las que permiten hacer administración de parches y actualizaciones de software. Así, habiendo mencionado que 2017 fue histórico en cuanto a la cantidad de vulnerabilidades reportadas, surge como un aspecto esencial para la protección tener las herramientas que permitan mantener los parches y las actualizaciones al día.

El elevado número de vulnerabilidades reportadas se encuentra acompañado del crecimiento en la cantidad de dispositivos IoT Internet

de las cosas (en inglés, Internet of *Things*, abreviado IoT; IdC, por sus siglas en español), concepto que se refiere a la interconexión digital de objetos cotidianos con Internet.

Alternativamente, en seguridad digital la constante implementación del Internet de las cosas, que es la conexión de Internet con más objetos que con personas, seguirá llamando la atención a una mejora continua de los procedimientos, esto debido a su capacidad de procesamiento, pues pueden ser utilizados para realizar algún tipo de ataque o acceder a las redes a las que están conectados, además, porque la fuga de información fue un incidente bastante recurrente durante los últimos años.

Bajo los aportes anteriores, un llamado de atención y de importante inversión es necesaria en las empresas del sector mixto privado, la supervivencia es un reto que de solo mirar hechos ocurridos como en Chile, donde recientemente se dio a conocer el caso de una estafa informática que afectó al Banco de Chile y donde un empleado realizó durante al menos un año transferencias no autorizadas por valor de 475 millones de pesos chilenos (cifra que supera los 700 mil dólares) simulando que se trataba de actividades laborales; y banco en el cual cabe destacar que se mencionaba entre las noticias por ciberataque, que también sufrió el 24 de mayo de 2018 un importante robo y en el que cibercriminales internacionales se llevaron mediante transferencias bancarias, cerca de 10 millones de dólares en lo que fue una operación sofisticada que incluyó la introducción de un código malicioso.

¿Entonces qué sumar a esta importante reflexión?

¿Existen las amenazas internas?

Cuando se habla de medidas de seguridad, no solo se refiere a las que se deben tener en cuenta para evitar ataques a la seguridad digital provenientes del exterior, sino también del interior de la empresa, organización o institución. Y es que puertas para adentro, una entidad, como puede ser en este caso un banco o cualquier entidad que maneje dineros o transferencias, debe tomar las precauciones suficientes ante la posibilidad real de que exista una amenaza interna.

La ciberseguridad ha pasado de ser arbitraria y atemorizante, a ser un enemigo casi estándar en el arte de los negocios modernos. Ahora que la mayoría de las organizaciones han aceptado el axioma que algún nivel de vulnerabilidad de datos es universal, muchos se están graduando en una era de comprensión, preparación y receptividad.

Cómo se ejecutan en estas variables se ha convertido en una característica distintiva entre los que están listos para lo inevitable y para aquellos que están destinados a ser noticia de primera plana. Las organizaciones pueden tomar una amplia variedad de pasos o decisiones, que abarcan políticas, educación, liderazgo y tecnología, para combatir una amenaza que ha cautivado tanto a las comunidades profesionales como a las comerciales.

En este sentido, la realización de auditorías internas es una gran herramienta para establecer un diagnóstico acerca del estado de la seguridad de cara a las puertas adentro de la organización, la siguiente recomendación suma a importante medida de prevención.

Constante migración al mundo digital con interés y preparación hacia las nuevas amenazas digitales

Mencionar entonces que el conglomerado de organizaciones migran actualmente a lo digital, es una realidad y por ende bajo las premisas de la Organización de Estados Americanos OEA, que en pasado Reporte de seguridad Cibernética e Infraestructura Critica de las Américas (2015) referente a las transformación y nueva generación industrial, explico que el interés de la comunidad de la seguridad para analizar y descubrir nuevas vulnerabilidades de los sistemas de automatización industrial, en particular de las infraestructuras críticas, ha crecido rápidamente.

Si bien este interés comenzó en casi todas las conferencias de seguridad importantes de 2013 y 2014, se ha hablado mucho de los ataques perpetrados contra los sistemas de control y automatización.

También se ha publicado mucho sobre este tema; asimismo, los proveedores están adaptando sus tecnologías para brindar "nueva" protección a estos sistemas. Sin embargo, lo más importante es el hecho de que los principales medios de comunicación han reportado un número

importante de ataques que afectan principalmente a la producción y distribución de petróleo, gas y energía.

Y América Latina no ha sido la excepción; existe un gran interés por investigar las posibles debilidades y los ataques sufridos. Los países latinoamericanos han estado siguiendo esos temas muy de cerca, aunque tienen menores presupuestos que los de los países europeos y Estados Unidos.