Ciberseguridad: el impacto más allá de las fronteras

Por Galo Torres
Miembro del Equipo Legal de la Asociación de Bancos Privados del Ecuador (Asobanca).

Haciendo un fugaz recorrido a través de la historia, el ser humano desde sus inicios ha tendido a buscar mecanismos que lo protejan y resguarden de los diversos peligros a fin de preservar sus intereses.

En el actual *boom* de la era digital, la información se ha constituido como el punto central sobre el cual giran las actividades de las diversas industrias. Para ello y con el objetivo de preservar su correcto desarrollo, estos actores han implementado mecanismos de protección tecnológica orientados a frenar y mitigar el impacto causado por terceros.

En la constante construcción de la arquitectura de seguridad que las industrias requieren, son importantes el desarrollo de análisis de riesgo respecto de la seguridad informática, a fin de establecer sus fortalezas y debilidades y, de esta forma, tener más control sobre los eventos, realizar monitoreos y coordinar estrategias para protegerse de los conocidos ciberataques.

Es aquí donde aparece el concepto de "Ciberseguridad" el mismo que, para el centro estadounidense National Initiative for Cybersecurity Careers and Studies (NICCS), *es la actividad o proceso, capacidad o estado por el cual los sistemas de información y comunicaciones y la información contenida en ellos están protegidos y/o defendidos*

En el mes de abril del presente año, las unidades de seguridad de empresas como Google detectaron alrededor de 18 millones de intentos diarios de ciberataques y más de 240 millones de mensajes de *spam* diarios.

contra daños, uso no autorizado, modificación o explotación. Definido de otra forma, la ciberseguridad debe ser reconocida como ese producto del desarrollo de la tecnología que ha obligado a las personas y empresas a construir sistemas digitales, enfocados a tutelar las diversas actividades económicas que practican.

La ciberseguridad se ha venido constituyendo como un tema cada vez más relevante en el desarrollo de las actividades empresariales y de las personas, haciendo que se destinen importantes recursos para hacer frente a los ataques perpetrados a sus diferentes escenarios o plataformas. En el contexto actual, se dice que las empresas que invierten en ciberseguridad son, sin duda, más seguras en caso de sufrir una afectación considerando que, año tras año, estos ciberataques se perpetran a un ritmo preocupantemente acelerado.

En los últimos años, según las estadísticas hay un aumento considerable de ataques perpetrados a diversos sectores como los gubernamentales, financieros, empresariales, entre otros. Según el "Reporte de Ciberseguridad 2020" elaborado por la OEA y el BID, América Latina y el Caribe no están lo suficientemente preparadas para hacer frente a los ciberataques. Este estudio refleja que únicamente *7 países de los 32 analizados en este reporte cuentan con un plan de protección de su infraestructura crítica y 20 han establecido algún tipo de grupo de respuesta a incidentes, llamado CERT o CSIRT según sus siglas en inglés*, limitando de esta forma la capacidad reactiva para identificar y responder a estos eventos en sus entornos.

Para tener una visión del impacto de los ciberataques, sólo durante el inicio de la pandemia, en el mes de abril del presente año, las unidades de seguridad de empresas como Google, detectaron alrededor de 18 millones de intentos diarios de ciberataques (entre los que se encuentran *malware* y *phishing* bancario) y más de 240 millones de mensajes de *spam* diarios. Por su parte, Microsoft detectó por cada día más de 60 000 mensajes con archivos o enlaces maliciosos vinculados a virus. Esto sólo por indicar un dato al inicio de la emergencia sanitaria global. ¡Imagínense las cifras a la fecha actual!

Los expertos señalan que, mientras los negocios o actividades económicas son de mayor relevancia o magnitud, existen más probabilidades de que sufran ataques. Sin embargo, no debe quitarse la atención a los impactos que sufren las pequeñas y medianas empresas, pues también están en latente riesgo. Es preocupante y alarmante el nivel de afectación financiera,

física y de orden legal cuando se producen estos impactos a los negocios que, en gran medida, pueden ser devastadores.

Sin duda este 2020 se ha configurado como un año atípico en los diferentes escenarios, dentro del cual también se encuentra el tema de la ciberseguridad tomando en cuenta que, a raíz de la pandemia del COVID-19, se han presentado una gran cantidad de amenazas de seguridad, ciberataques y brechas de datos que han afectado tanto a las empresas, a las entidades gubernamentales y, por supuesto, a los clientes y usuarios de servicios. Se destaca de estos eventos la capacidad que tienen los ciberdelincuentes de adaptarse a las nuevas realidades y circunstancias, como siempre lo hacen, modificando de este modo los impactos y ataques hacia los diferentes entornos en los cuales el ser humano se desarrolla.

Esta crisis sanitaria originada por el COVID-19 ha denotado que la ciberdelincuencia, presente y ejerciendo acciones en diversos puntos del planeta, se encuentra aprovechando todo tipo de vulnerabilidades del universo de usuarios de los diferentes sistemas de redes, obteniendo resultados de éxito con estas actuaciones ilegales y maliciosas. Por citar un caso reciente, en Chile en plena pandemia, se presentó un ciberataque a la infraestructura de seguridad de la industria financiera, específicamente un ataque al Banco del Estado de Chile (conocido con el nombre comercial BancoEstado), el cual provocó como resultado un posible secuestro de datos, siendo un hecho sin precedentes en esta nación.

Si bien en el caso del Ecuador, hasta la presente fecha no ha habido ataques de alta incidencia como en México o Chile, el riesgo siempre estará latente ante estos eventos. Esta estadística no tan alarmante en el país es producto de las importantes inversiones realizadas en ciberseguridad, en especial desde el sector privado que ha direccionado esfuerzos para proteger sus infraestructuras tecnológicas, incluso efectuadas antes del aparecimiento de la pandemia; acciones que han permitido a los actores ser más reactivos para enfrentar esta problemática en el ciberespacio.

Resumiendo lo tratado, la ciberseguridad se configura como ese elemento trascendental en los negocios digitales, a través del cual se busca mitigar los riesgos que toda actividad económica que incursiona en la red pueda tener. Resulta que toda industria es blanco de ataques cibernéticos y América Latina no ha sido la excepción, en especial en los últimos tiempos con el apogeo de la pandemia, durante la cual las entidades gubernamentales y las grandes corporaciones han sido afectadas a través de hackeos o *phishing*, por enunciar algunos casos acontecidos.

Para Latinoamérica y el Caribe se constituyen como retos para la ciberseguridad fomentar la coo-

peración entre los Estados, de igual forma el involucramiento de todos los actores relevantes, públicos y privados, así como el establecimiento de mecanismos de análisis, verificación y de monitoreo de los impactos originados por este tema, compartidos a nivel local, así como también a escala regional. En línea de esto, es importante consolidar una cultura de gestión para estos eventos que permita hacer más efectiva y óptima la ejecución de acciones en los diferentes escenarios, canalizando para ello la vinculación de todos los actores del sector público y del sector privado.

Por otra parte, su objetivo no sólo se dirige a la prevención sino también se enfoca a generar confianza hacia los usuarios o beneficiarios de un servicio, contribuyendo de esta forma al interés en los diferentes mercados y a la disminución de los riesgos de exposición que pudieran sufrir los consumidores y los sistemas implementados.

EL AUTOR

Galo Alejandro Torres Proaño es abogado por la Universidad Internacional SEK, máster en Derecho Financiero Bursátil y Seguros por la Universidad Andina Simón Bolívar y especialista en Derecho Financiero Bursátil por la Universidad Andina Simón Bolívar. Actualmente forma parte del Equipo Legal de la Asociación de Bancos Privados del Ecuador (Asobanca).