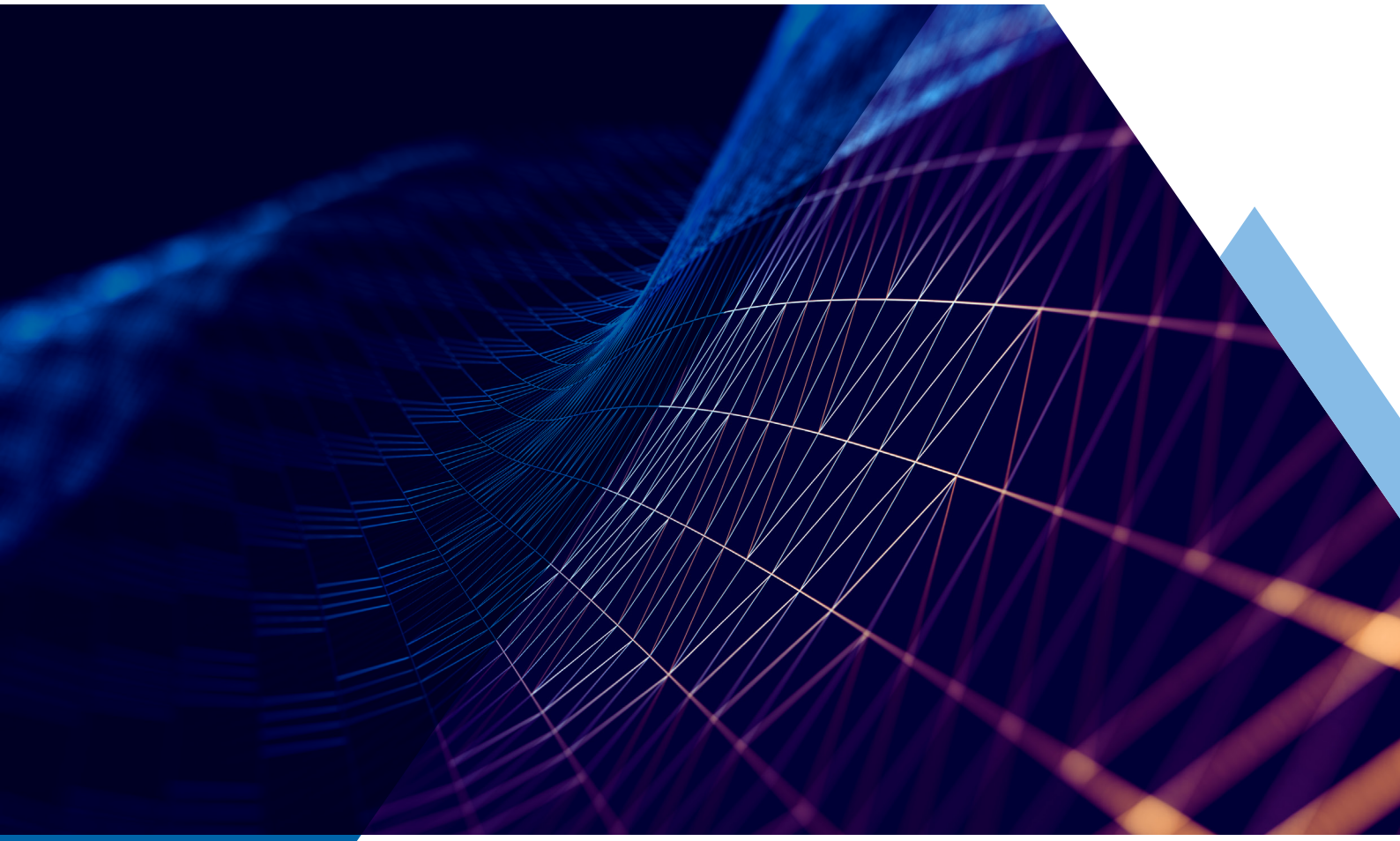
INTERNATIONAL CHAMBER OF COMMERCE
The world business organization



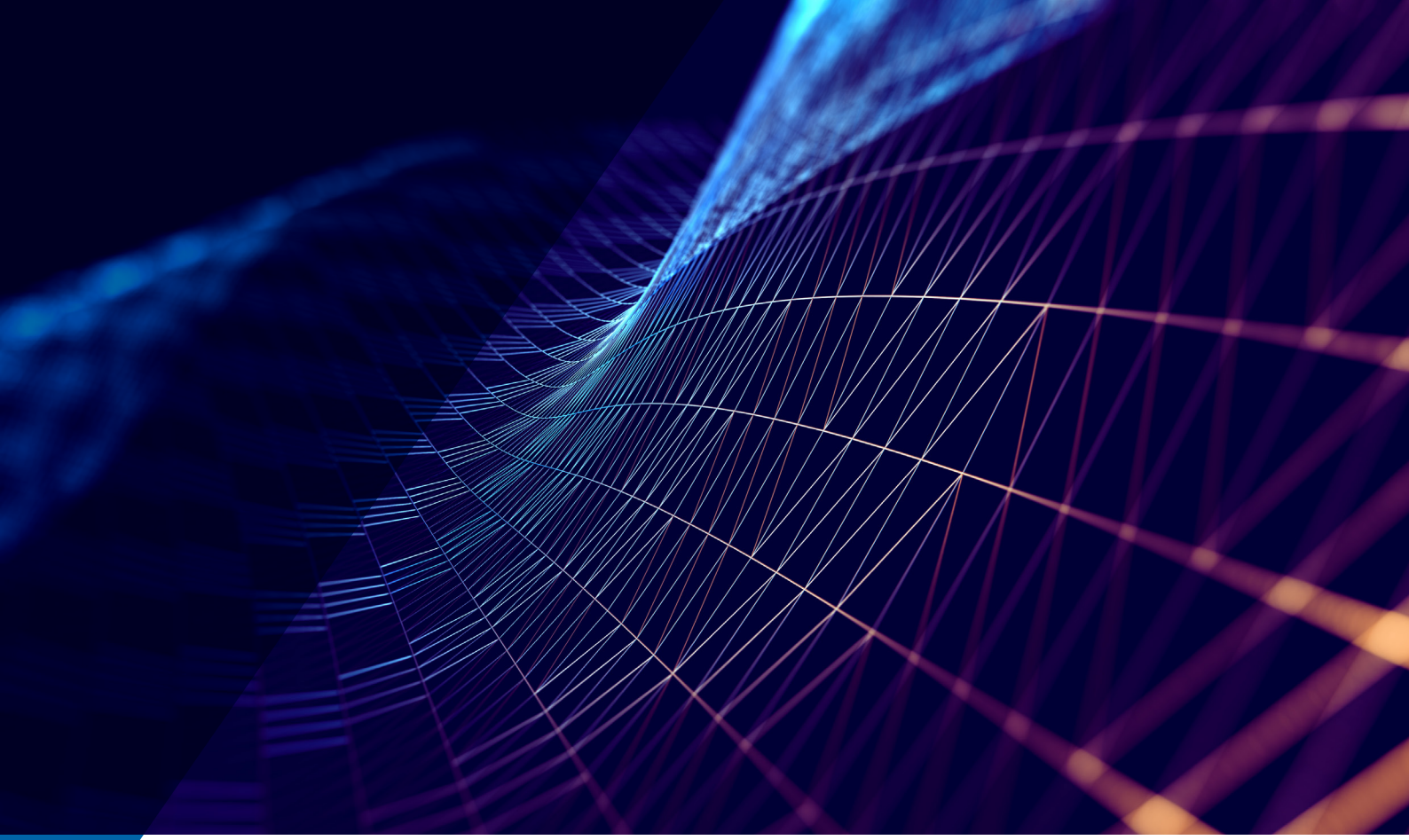
ICC MANUAL DE LA POLÍTICA SOBRE

Ciberseguridad

Traducción realizada al español con el apoyo de:

ICC MEXICO INTERNATIONAL CHAMBER OF COMMERCE

Microsoft



ÍNDICE

INTRODUCCIÓN

El sector privado ha asumido, y continúa asumiendo roles y responsabilidades significativas en el desarrollo de tecnologías de la información y la comunicación (ICTs). Como representante de 45 millones de compañías de todos los tamaños, y en todos los sectores, en más de 100 países, la Cámara Internacional de Comercio (ICC), está comprometida en asegurarse de que las tecnologías digitales trabajen para todos, todos los días, en todo lugar, para poder lograr el potencial total de la economía digital, así como salvaguardar el adecuado funcionamiento de las infraestructuras críticas. En tanto que lo anterior siempre fue un objetivo importante, en el contexto actual de la pandemia COVID-19 esto es fundamental, ya que redes digitales seguras, confiables y resistentes, son vitales para mantener el funcionamiento adecuado de nuestras economías y sociedades, así como para proteger vidas y formas de subsistencia en todo el mundo.

La ICC trabaja con gobiernos y negocios a nivel mundial, para generar un entendimiento común respecto de lo que constituye una política robusta sobre ciberseguridad, derivado de la proliferación/constantemente creciente oleada de ataques, y mejores prácticas para poder promover una internet más segura para los negocios y los usuarios.

Con una historia de cien años en el desarrollo de reglas aplicables y reconocidas globalmente, al reunir expertos y practicantes, la ICC considera esencial que los negocios y los gobiernos cuenten con un entendimiento compartido respecto del como conceptualizar los riesgos, los objetivos, los impactos y las respuestas de ciberseguridad, incluyendo leyes y reglamentos nacionales e internacionales. En tanto que los gobiernos y los negocios tienen diferentes roles al enfocarse en la ciberseguridad, éstos se refuerzan unos a los otros.

El presente manual de la política resalta algunos de los temas principales que los negocios y la sociedad están enfrentando. La Parte 1 del documento, presenta una lista no exhaustiva, como un punto de partida en la identificación de los temas principales, para que todos los participantes puedan trabajar en conjunto encaminados a soluciones efectivas. La Parte 2 del documento, describe áreas clave donde la ICC y sus miembros, desarrollarán documentos adicionales para proveer consideraciones adicionales, herramientas prácticas y recomendaciones de políticas para los actores, tanto del sector privado, como el público.

CONTEXTO: El impacto de las amenazas cibernéticas en los negocios

Con daños relacionados con la ciberseguridad proyectados a alcanzar $6 trillones anualmente en el 2021[1], los negocios, los legisladores y los usuarios, luchan para mantenerse al día con las amenazas en línea, mismas que evolucionan rápidamente. Hoy, el crimen cibernético impacta a todos los negocios, sin importar su tamaño, o industria, o ubicación geográfica, con alrededor de 50% de todos los ataques cibernéticos siendo cometidos en contra de pequeñas y medianas empresas (PYMEs).[2]

La economía digital, el internet, y el flujo transfronterizo de datos que le dan soporte, ya dieron cuenta de un crecimiento considerable en el PIB en muchos países.[3] Discutiblemente, el mayor impacto económico de la economía digital deriva de la digitalización de procesos tradicionales de la industria, conforme compañías a lo largo de todos los sectores buscan utilizar la tecnología para mejorar sus operaciones y modelos de negocios.[4] Sin embargo, el crimen cibernético amenaza con frustrar el potencial impacto económico de ICT y digital, conforme los consumidores y los negocios expresan una preocupación respecto de la ciberseguridad.[5]

Conforme la pandemia COVID-19 se expandió a todo el mundo, muchas organizaciones comenzaron a mover grandes partes de sus operaciones a que fueran en línea, para poder así

---

1 Cybersecurity Ventures (2020), Cybercrime Report
2 Cybersecurity Ventures (2017) *Cybercrime Report*
3 McKinsey (2011) *The great transformer: The impact of the Internet on economic growth and prosperity*
4 UNCTAD (2017) *World Investment Report 2017: Investment and the Digital Economy.*
5 Mckinsey (2015) *Digitizing the value chain*

asegurar la continuidad de sus negocios, proteger a sus trabajadores y continuar brindando servicios a sus clientes. Como consecuencia de esta crisis, ha habido un aumento en el uso de herramientas en línea y digitales, que crearon y, continúan creando, nuevas oportunidades para que los actores maliciosos se aprovechen de los efectos disruptivos de la crisis y ataquen a los negocios, especialmente PYMEs por ataques cibernéticos.

Aún antes de la crisis actual, el impacto de los ataques cibernéticos era una preocupación creciente. En el 2019, el costo promedio de una filtración de datos fue de USD$3.92 millones.[6] Un reporte reciente sugiere que los pequeños negocios son el objetivo de más del 40% de los ataques cibernéticos, con una pérdida promedio por cada ataque de más de USD$188,000.[7] Pero el costo de una filtración de datos para los negocios va más allá de un daño monetario, ya que la pérdida de secretos industriales, información privilegiada, o el daño a la reputación comercial pudieren amenazar, o destruir un negocio en su conjunto.[8] En los Estados Unidos, 60% de las PYMEs se encuentran en quiebra dentro de los seis meses siguientes a un ataque cibernético.[9] Conforme los negocios a lo largo de toda la economía tradicional, desde la manufactura hasta la energética, buscan digitalizar sus operaciones, como una forma de incrementar su competitividad, esto provee nuevas oportunidades para que el crimen cibernético se expanda, especialmente ya que actores-estado y no de estado buscan cada vez más, atacar e interrumpir la infraestructura y los sistemas críticos.[10]

La naturaleza sin fronteras del internet, la economía digital, creciente interdependencia ciber-física por medio del IoT y el crimen cibernético, pintan una imagen legal y operativa compleja para la ciberseguridad. Casi todos los sectores utilizan ICT y dependen del internet para todo, desde las tareas más simples, hasta las más estratégicas. Las cadenas de suministro globales están interconectadas cada vez más, y los sistemas ICT a lo largo de esas cadenas de suministro tienen dispositivos internos y externos que pretenden facilitar las operaciones de los negocios. Sin embargo, estos sistemas interconectados crean un paisaje complejo en el que combatir el crimen cibernético puede ser particularmente desafiante, conforme los actores maliciosos pueden explotar fácilmente las vulnerabilidades en los procesos de negocios y atacar empleados en lo individual, a lo largo de todas las partes de la cadena de suministro. Adicionalmente a los riesgos operativos y de comportamiento, las manifestaciones técnicas de los ataques cibernéticos, desde Malware hasta Ransomware, hasta ataques cibernéticos a la cadena de suministro, evolucionan constantemente.

Adicionalmente, un incremento gubernamental en la inversión en capacidades cibernéticas avanzadas ha impulsado en gran parte, la escalada de ataques sofisticados.[11] Los reportes sugieren que más de 60 países actualmente se encuentran desarrollando dichas capacidades[12] conforme la comunidad de negocios continúa estando expuesta a amenazas cibernéticas serias y crecientes de actores-estado.[13] El espionaje patrocinado por los estados ha ido en crecimiento, con 20% de los negocios mundiales calificándolo como el riesgo más serio para sus negocios.[14] Muchos de los ataques cibernéticos más sofisticados, han sido atribuidos directamente a los Estados o a los actos de sus representantes. Inclusive los ataques realizados por actores maliciosos independientes son muchas veces una consecuencia de la actividad de un gobierno, ya que las capacidades cibernéticas proliferan rápidamente cuando éstas son robadas, vendidas o de otro modo readaptadas a los propósitos criminales. Estamos viendo, cada vez más, poderes cibernéticos avanzados colocados en la parte más alta de la pirámide de actores maliciosos, con sus herramientas y tácticas proliferando hacia abajo y a un ecosistema peligroso de actores perniciosos afiliados y no afiliados con objetivos políticos y criminales.

---

6 Ponemon (2019) *Cost of a Data Breach Report*
7 Verizon (2019) Data Breach Investigation Report
8 Eubanks (2017) The True Cost Of Cybercrime For Businesses. *Council Post*; Ponemon (2016) *Cost of Cyber Crime Study & the Risk of Business Innovation*
9 Miller (2016) 60% of small companies that suffer a cyber attack are out of business within six months. *Denver Post.*
10 McKinsey (2019) *Unlocking the value of digital operations in electric power generation;* UNCTAD (2017) *World Investment Report 2017: Investment and the Digital Economy*
11 Hi-Tech Crime Trends 2018. Group-IB. Oct. 2018. https://www.group-ib.com/media/hi-tech-crime-trends-2018/
12 Valantino-DeVries, Jenniter, Lam Thuy Vo, Danny Yadron. *Cataloging the World's Cyberforces.* Wall Street Journal. http://graphics.wsj.com/world-catalogue-cyberwar-tools/
13 Council on Foreign Relations (n.d.) State-sponsored cyber operations tracker
14 Businesswire (2017) Cyber Espionage Tops the List as Most Serious Threat Concern to Global Businesses in 2017

Al mismo tiempo, cuando se trata de ataques cibernéticos, hay asimetrías significativas entre los delincuentes y los protectores respecto de sus habilidades, herramientas y costos. De 10,000 ataques, el protector tiene que estar en lo correcto 10,000 veces, en tanto que el delincuente, solamente una vez, para tener éxito. Los delincuentes, muchas veces, cuentan con una caja de herramientas más grande y mejor equipada, comparado con las capacidades de defensa de los negocios (especialmente PYMEs) y usuarios. El crimen cibernético tiene un alto porcentaje de pago, con costos relativamente bajos del atacante, en tanto que los gastos de la defensa cibernética son considerablemente más altos. Por lo tanto, los negocios, los consumidores y los usuarios de tecnología están librando una batalla perdida, sin el apoyo de los gobiernos tanto en el plano nacional como en el internacional.

Ni los negocios ni los gobiernos pueden combatir estas amenazas sin fronteras por si solos.

La ciberseguridad es una actividad de recursos intensivos, requiriendo de reservas tanto del sector privado como el público. Conforme los negocios y los reguladores buscan encontrar formas significativas para mitigar las preocupaciones sobre la ciberseguridad, se requiere de una colaboración para poder generar conciencia respecto de las vulnerabilidades e incidentes, así como para incrementar la resiliencia en contra de amenazas cibernéticas complejas y sin fronteras.

El sector privado depende de una política y un ambiente regulatorio seguro, estable y confiable, para alentar las oportunidades, estimular la innovación y crear valor para las comunidades. Los actos que perjudican este ambiente favorable supone una amenaza, no solamente a la seguridad, si no también al desarrollo económico y a las formas de subsistencia. Por lo anterior, es imperativo que la industria forme parte de las discusiones internacionales de políticas sobre ciberseguridad, por dos principales razones.

Primera, una interpretación común de las leyes internacionales y las normas es necesaria para asegurar una certeza jurídica y la predictibilidad del comportamiento de los estados, lo que a su vez, tiene un impacto significativo en las decisiones de inversión y en los riesgos que las compañías pueden cuantificar en sus operaciones multinacionales.

Segunda, debido a la naturaleza sin fronteras y la interconectividad tanto de la economía digital como de las amenazas cibernéticas, los acercamientos nacionales a la ciberseguridad requieren de acuerdos y cooperación internacional para que funcione adecuadamente.

Se requiere de resultados tangibles e indicadores concretos que reflejen de manera objetiva, un comportamiento responsable de los estados en el ciberespacio. En tanto que los temas importantes respecto de los procesos y normas que pretenden proveer conductos y mecanismos para lograr resultados continúan siendo esenciales, existe una necesidad urgente de mejoras medibles en el medio. Definir resultados, indicadores y procedimientos de seguimiento, a corto y largo plazo, es crítico. El sector privado tiene un lugar privilegiado para informar a los legisladores respecto de los usos y los efectos deseados de dichas medidas, así como para señalar las potenciales barreras que pudieren impactar en su implementación.

PARTE 1: RETOS ACTUALES EN LA CIBERSEGURIDAD

La falta de un conocimiento común de las amenazas y conceptos de la ciberseguridad

El impacto de un ataque cibernético varía significativamente debido a la naturaleza del actor, el motivo, el objetivo y la categoría de la amenaza, así como de la frecuencia, el grado de éxito de un incidente y la severidad de las consecuencias. Uno de los retos de alentar acercamientos integrales a la ciberseguridad, es la falta de definición y un conocimiento común de los tipos de amenazas. Esta complejidad, y un ambiente en constante cambio, hace que el conceptualizar las amenazas sea difícil, fragmentando acercamientos a la ciberseguridad y, por lo tanto, contribuir a un ambiente donde el crimen cibernético pueda prosperar.

La falta de una interpretación común y efectiva de las normas y leyes

En abordar de forma colaborativa el crimen cibernético es importante para crear una resiliencia cibernética global y efectiva. Aún y cuando ha habido algunas declaraciones internacionales y bilaterales para restringir los ataques cibernéticos que se enfocan en empresas e infraestructura crítica, el progreso en el desarrollo y la adopción de normas internacionales que regulen y vinculen a los estados a un comportamiento responsable en el ciberespacio, ha sido lento.[15]

A nivel internacional

Aún y cuando, muchos están de acuerdo que las leyes fuera de línea, también deberían de aplicar en línea, actualmente existen grandes diferencias entre los estados, respecto de la interpretación, aplicabilidad e implementación de la legislación internacional. Sin un entendimiento común, respecto de cómo es que la legislación internacional, en su totalidad, es aplicada en el ciberespacio, hay muy poca esperanza para definir y hacer valer la rendición de cuentas por el comportamiento en el ciberespacio de los Estados responsables, y como consecuencia, será imposible mejorar el paisaje de confianza para todos los involucrados.

La cooperación trasfronteriza respecto del crimen cibernético también enfrenta sus propios retos, ya que no cuenta con una investigación y persecución criminal efectiva trasfronteriza que sea consistente con la legislación y tratados internacionales, acuerdos y mecanismos internacionales de cooperación. Los acuerdos y los mecanismos internacionales de cooperación, muchas veces pueden ser una forma efectiva para lidiar con el crimen cibernético que cruce fronteras. Actualmente, la Convención sobre Cibercriminalidad del Consejo Europeo (Convención de Budapest) es el único instrumento internacional vinculatorio sobre crimen cibernético, enfocado en la facilitación de este nivel de cooperación. Los Tratados de Asistencia Jurídica Mutua (TAJM), ya sean bilaterales o regionales, proveen otro mecanismo para permitirle a las fuerzas policiales acceso a datos en otras jurisdicciones con una mayor eficiencia. Al respecto, la Convención Sobre Crimen Organizado Transfronterizo también tiene un papel importante que jugar.

A nivel nacional

Los negocios se basan en el apoyo del gobierno para asegurar que las leyes necesarias estén vigentes para que las actividades de crimen cibernético sean ilegales. Los gobiernos deben asegurar una criminalización similar de crímenes cibernéticos específicos y de crímenes cometidos en el ciberespacio, para evitar la creación de ´paraísos cibernéticos´.

La falta de cooperación o conciencia de esfuerzos similares a través de jurisdicciones y regiones plantea retos adicionales para el alineamiento de políticas y regulaciones, que pudieren ayudar a reducir la incertidumbre y alentar la confianza en el ecosistema digital.

Deficiencias en la capacidad y las medidas de generación de confianza

Los usuarios primerizos y ciertas demografías (ej. menores, mujeres) muy frecuentemente se ven afectados por el impacto del crimen cibernético, ciberbullying y otros riesgos cibernéticos. Estos grupos y todos los demás usuarios del internet necesitan poder identificar los riesgos y administrar las amenazas de forma efectiva para aprovechar las oportunidades que el internet ofrece.

Desde una perspectiva de negocios, es vital que una compañía –grande o pequeña, en línea y física o de alta tecnología–, sea capaz de identificar su riesgo en seguridad cibernética y administrar de manera efectiva las amenazas a sus sistemas de información. Al mismo tiempo, todos los gerentes de negocios, desde los directores de pequeños negocios familiares, hasta los ejecutivos de grandes compañías multinacionales, deben de reconocer que, la seguridad absoluta es un objetivo elusivo.

A diferencia de muchos retos de negocios, la administración del riesgo de la seguridad cibernética continúa siendo un problema, sin un remedio simple disponible.

---

15 El Grupo de Expertos Gubernamentales es un grupo regulado por las Naciones Unidas, enfocado en el avance de un comportamiento responsable de los Estados en el ciberespacio, en el contexto de seguridad internacional, que ha estado trabajando desde el 2004. Ver, la Resolución 73/266 de UNGA.

Una dimensión crítica a considerar, es que muchos países en desarrollo requieren y necesitan asistencia técnica para crear la infraestructura legal y regulatoria relacionada, para dar soporte al desarrollo de un ambiente digital seguro, confiable y basado en reglas. La necesidad continúa siendo mayor: demasiados países aún no cuentan con un CERT, protección de datos en su legislación, legislación sobre ciberseguridad vigente o estrategias cibernéticas nacionales—y la infraestructura técnica y práctica relacionada que es esencial para apoyarlas.

El escalofriante efecto de las respuestas regulatorias desproporcionadas

Las cadenas de suministro de la ICT son globales. La integración e interdependencia son aspectos clave del ambiente digital que se basa en reglas compatibles entre jurisdicciones nacionales y los flojos de datos globales para trabajar sin contratiempos.

Adicionalmente, se requiere de una cooperación y de esfuerzos para desarrollar prácticas destinadas a asegurar se de que las medidas de ciberseguridad no solamente provean la protección necesaria, si no que también permitan las innovaciones impulsadas por datos. Los flujos de datos globales transfronterizos permiten tanto e crecimiento económico, como beneficios sociales. El implementar medidas cibernéticas que, de forma desproporcionada, restrinjan los flujos de datos transfronterizos, o reduzcan el acceso al mercado, podrían impactar de forma negativa el comercio, la inversión o la innovación.

La seguridad es un elemento esencial de la confianza en tecnologías nuevas y emergentes, y un factor que pudiere impactar a cualquier organización conectada al internet, más no es una solución unitalla. Y por lo tanto no es apropiada para una determinación angosta y vertical. Conforme nuevas tecnologías continúan desarrollándose y emergiendo, las implicaciones de ciberseguridad, requieren de una consideración caso por caso.

PARTE 2: RESPONDIENDO A LOS RETOS EN CIBERSEGURIDAD

Para poder atender los retos antes mencionados, la ICC recomienda que todos los involucrados:

- trabajen en conjunto para desarrollar un entendimiento común entre los actores de el sector privado como del público (a niveles nacionales e internacionales) de las amenazas, los actores y los acercamientos a la ciberseguridad;
- reconocer que la legislación internacional aplica en su totalidad al ciberespacio; basado en esta premisa, los gobiernos, consultando a todos los involucrados, se deben de adherir a las normas internacionales acordadas, así como desarrollar mecanismos para implementar eficientemente dichas normas y considerar, cuando sea apropiado, el desarrollo de nuevas normas internacionales y/o legislación nacional.
- trabajar hacia la introducción y aplicación de una política criminal nacional enfocada a la protección de los negocios y la sociedad, de crímenes cibernéticos.
- reconocer la importancia de una mayor cooperación entre los gobiernos nacionales, en el combate al crimen cibernético, con una cooperación funcional y a la medida respecto de asuntos criminales.
- trabajar en conjunto para avanzar en la ampliación de la capacidad y las medidas de generación de confianza; y
- considerar las medidas y estándares respecto de ciberseguridad, conforme se relacionan con tecnologías existentes y emergentes en específico, caso por caso, de conformidad con las normas y leyes internacionales, por medio de un acercamiento basado en el riesgo.

Conceptualizando las amenazas cibernéticas, los actores y las respuestas

Al asegurar sus propios activos y operaciones y al tomar los pasos para proteger a sus usuarios y clientes, los negocios cada vez más entienden la importancia de implementar procesos holísticos de administración del riesgo de la ciberseguridad. Los negocios constantemente desarrollan y lanzan medidas diseñadas para asegurar la seguridad de las redes, los usuarios de productos, proteger dispositivos y proteger el contenido que se almacena en estas redes de un ataque. Dichas medidas incluyen actividades para no solamente identificar y mitigar riesgos de ciberseguridad, sino también para detectar, responder y recuperarse de incidentes o eventos de ciberseguridad.

Debido a la constante amenaza y respuestas a los ataques cibernéticos, el enfoque de los negocios hacia la ciberseguridad sola mente puede llegar hasta cierto punto, y una cooperación efectiva público-privada es esencial para fortalecer la seguridad en internet, y responder a el alto y creciente rango de amenazas de ciberseguridad al internet global. Es esencial que los negocios y los gobiernos tengan un entendimiento compartido de como conceptualizar las amenazas, los impactos y las respuestas respecto de la ciberseguridad.

Los acercamientos a la ciberseguridad deben de ser holísticos y consistentes a lo largo de los sectores, y reconocer interdependencias críticas tanto en el contexto nacional como en el internacional. Conforme los gobiernos buscan promover y asegurar un uso suficiente de acercamientos efectivos a la administración del riesgo cibernético, deben de estar conscientes de esfuerzos similares a través de jurisdicciones y regiones y buscar el alinear políticas y regulaciones hasta el límite más amplio que sea aplicable.

Acercamientos globalmente alineados a la administración del riesgo cibernético pueden facilitar la interoperabilidad y mejorar la visibilidad y el entendimiento entre entidades que tengan operaciones transfronterizas. Por lo anterior, es importante que los negocios y los gobiernos tengan un entendimiento compartido de como conceptualizar las amenazas, los impactos y las respuestas respecto de la ciberseguridad. La Figura 1 ayuda a navegar por medio de un acercamiento común a la ciberseguridad.

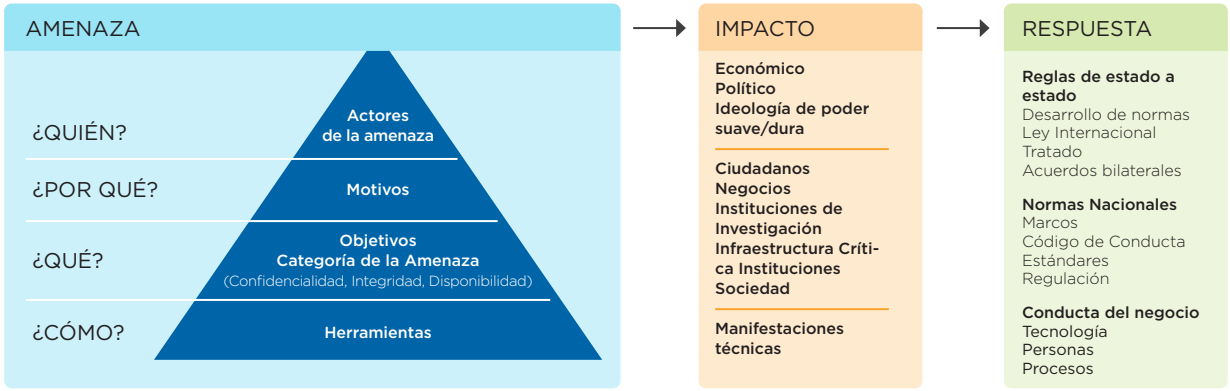


Figura 1 *Un acercamiento común a la ciberseguridad*

Desarrollando e implementando normas compartidas

En tanto que los negocios deben de ser proactivos en asegurar sus propios activos y operaciones y al tomar los pasos para proteger a sus usuarios y clientes, también deberían de poder contar con el apoyo de los gobiernos para asegurarse de que las leyes necesarias se encuentran vigentes e implementadas para garantizar que ciertos eventos de ciberseguridad sean ilegales.

Con esto en mente la ICC, urge a los gobiernos para que implementen y se adhieran a las normas que previamente se han acordado en las discusiones de las Naciones Unidas, así como a que desarrollen mecanismos para implementar de manera efectiva dichas normas.

Como un primer paso, los gobiernos deberían de comenzar por cumplir con las normas internacionales establecidas y/o, que se requieran para incrementar la claridad, desarrollar normas y prácticas globalmente reconocidas en colaboración con los actores relevantes. Por ejemplo, los gobiernos pueden:

- Desarrollar normas internacionalmente reconocidas que promuevan un ecosistema estable, en colaboración con la industria.
- Mejorar el entendimiento de, y un consenso, respecto de las formas en que la legislación internacional existente rige el comportamiento en línea del estado.
- Sustentar los acuerdos previos con normas para proveer un mapa para su discusión futura, y el establecimiento de estándares más específicos que protejan los flujos transfronterizos de datos, así como la libre expresión. Esto también debería de incluir el compromiso de los estados de prevenir de manera constante cualquier forma de crimen cibernético que emane de su territorio, y prohibir el uso ofensivo del ciberespacio por los actores Estado en momentos de paz, incluyendo el robo de la información confidencial de los negocios y la interrupción de la infraestructura crítica, mediante el ciberespacio y patrocinado por un estado[16].

Los negocios apoyan las normas acordadas por el Grupo de Expertos Gubernamentales de las Naciones Unidas en 2015, y esperan poder contribuir con su implementación y para reforzar aún más estas normas.

Adicionalmente, el sector privado ya ha apoyado, colaborado en, y lanzado iniciativas para promover normas ambiciosas para el uso responsable de la tecnología, tales como el Foro Global Sobre la Experiencia Cibernética, el Acuerdo de Tecnología sobre Ciberseguridad, El Llamado de Paris sobre la Confianza y la Seguridad en el Ciberespacio o la Iniciativa de la Sociedad en Internet MANRS, por nombrar algunos. Continuaremos apoyando este trabajo en el futuro y apoyaremos el intercambio de información y la cooperación entre dichas iniciativas.

Cuando se trata de combatir el crimen cibernético, los gobiernos pueden implementar mecanismos para coordinar los esfuerzos de las fuerzas policiales internacionales y facilitar la investigación y los procesos de extradición. La Convención de Budapest es el único instrumento internacional vinculante específico sobre el crimen cibernético, y los Estados deberían de considerar convertirse en signatarios de la Convención de Budapest, o en utilizarla como una guía para desarrollar una legislación nacional integral. Los estados también deberían de aprovechar la Convención Sobre Crimen Organizado Transfronterizo para mejorar la asistencia legal mutua con relación al crimen cibernético. Los gobiernos también pueden considerar el establecer Tratados de Asistencia Jurídica Mutua (TAJM) bilaterales o regionales, que permitan y faciliten la cooperación transfronteriza para la aplicación de leyes, y al mismo tiempo mantener suficientes protecciones de privacidad y seguridad.

Conforme los gobiernos buscan promover o asegurar un uso suficiente de acercamientos efectivos a la administración del riesgo cibernético, deben de ser conscientes de esfuerzos similares a lo largo de jurisdicciones y regiones y buscar alinear las políticas y regulaciones hasta el límite más amplio posible. Dichos acercamientos también aseguran que todas las organizaciones locales puedan acceder a las mejores tecnologías, servicios y ofertas de seguridad de su clase, y expandir sus operaciones, ya sea mediante un crecimiento directo a lo largo de diferentes mercados o mediante su integración a ofertas de proveedores transfronterizos.

Aumentando la capacidad de generación

Una mayor conciencia respecto de la ciberseguridad y el conocimiento de como proteger redes puede fortalecer no solamente a los individuos, a los negocios, a las comunidades, sino también la capacidad de todo un país para proteger la infraestructura digital crítica y combatir las amenazas cibernéticas. Esto nunca había sido tan claro, como durante la crisis de COVID-19. La madurez de la capacidad respecto de la ciberseguridad en un país alienta la confianza en el ambiente en línea, y promueve el acceso significativo por parte de todos los grupos en una sociedad, por lo tanto, ayuda a atender la brecha digital.

La ICC tiene una orgullosa historia de cien años, de proveer a las compañías de herramientas y guías autorregulatorias para promover buenas prácticas de negocios. La Comisión de la Economía

16 Foro Económico Mundial: Reporte de Riesgos Globales 2018 http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

Digital de la ICC desarrolló una guía simple y clara en el 2015 para ayudarle a los negocios a que jugaran su parte al atender el reto, cada vez más serio, de la ciberseguridad. La Guía sobre ciberseguridad para los negocios de la ICC se integra de guías globales sobre ciberseguridad y estrategias nacionales, y presenta cinco principios que le ayudan a las empresas a identificar los riesgos de ciberseguridad, y tomando de diversas fuentes y mejores prácticas, adicionalmente identifica seis acciones clave que las compañías deberían de implementar.

La ICC también, recientemente se asoció con el Cyber Readiness Institute (CRI), una iniciativa sin fines de lucro que convoca a varios líderes de negocios de diversos sectores y regiones geográficas, para compartir recursos y conocimiento que provee información para el desarrollo de herramientas de ciberseguridad gratuitas para pequeñas y medianas empresas. Por medio de esta asociación, la ICC trabajará para poner a disposición el Programa de Preparación Cibernética a todos nuestros 45 millones de miembros, de todos tamaños y sectores alrededor del mundo, que estén buscando protegerse de amenazas digitales.

Dicho lo anterior, muchos países no cuentan con los fundamentos en su códice legal: no hay marcos de protección de datos en docenas de países; muchos no cuentan con un CERT/CSIRT, y la legislación sobre el crimen cibernético y otra legislación cibernética se encuentra obsoleta, o totalmente inexistente, en otros.[17]

Existe una necesidad de una generación de capacidad mucho mayor para asegurar una legislación básica y una infraestructura para construir una confianza cibernética y permitir la participación en los esfuerzos globales sobre ciberseguridad.

Aplicaciones y estándares sobre ciberseguridad

La confianza en la disponibilidad, confiabilidad y resiliencia de los sistemas de información y las redes, incluyendo el internet, deben continuar siendo fortalecidos para poder lograr al máximo un crecimiento económico alentado por ICT, y asegurar la operación fluida de los negocios a nivel global. Todos los actores deben de trabajar en conjunto para promover prácticas efectivas de ciberseguridad y el internet interoperable abierto, seguro, estable, resiliente y global.

Se deben de realizar esfuerzos tanto para resaltar la importancia del tema, así como para alentar la investigación, innovación y lanzamiento continuo de soluciones apropiadas para el contexto. Conforme las soluciones de seguridad se implementan, también se debe de poner atención para asegurar que las medidas de seguridad sean consistentes y apropiadas con los riesgos asociados y los resultados deseados, y considerar su inoperatividad a lo largo de varias implementaciones tecnológicas.

En una situación que requiere de una respuesta regulatoria a nivel nacional, esto se puede lograr proporcionalmente al primero, asegurar buenas estimaciones del impacto de los ataques cibernéticos a los negocios y a las sociedades. Segundo, cuando se consideren intervenciones regulatorias apropiadas (objetivo regulatorio) y efectivas (beneficio neto), esto se puede lograr proporcionalmente al balancear el impacto de los ataques cibernéticos, con los recursos privados y públicos requeridos para fortalecer la resiliencia a lo largo de toda la cadena de valor, ya que los costos pueden ser prohibitivamente caros para las pequeñas organizaciones.

Al considerar la legislación cibernética, los estados deben de tratar de balancear los beneficios del comercio, la inversión y la innovación, contra las preocupaciones reales respecto de la seguridad nacional. En casos raros los requerimientos de seguridad nacional requieren ser considerados, los Estados deben de buscar el implementar medidas que sean transparentes, predecibles, proporcionadas, y no una restricción velada al comercio.

Los estándares de ciberseguridad muchas veces son mejor logrados por medio de compromisos propios de los participantes del mercado, y diversas iniciativas y grupos de cooperación ya se

17 Para obtener mayor información, consultar el Contador de Legislación Cibernética Global que mantiene la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, en https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/summary-adoption-e-commerce-legislation-worldwide.

han establecido. Las pruebas de seguridad se deben de permitir, en una forma tal, que facilite la adopción de Criterios Comunes (ver, ej. https://www.commoncriteriaportal.org/) que sean consistentes con la legislación existente y aplicable. El acercamiento de estandarización común permite la adopción dinámica, para poder ajustar y tomar en consideración los cambios en tecnología, así como diversas amenazas y riesgos..

CONCLUSIÓN

Para lograr un resultado positivo, los gobiernos deben de colaborar con otros participantes para promover una cultura de seguridad, con una legislación adecuada vigente para combatir el crimen cibernético. De la misma manera, políticas adecuadas y marcos legales relacionados con la protección de datos y privacidad, también son esenciales para asegurar que los clientes y los ciudadanos puedan continuar confiando en los ICTs y utilizando servicios en línea.

La colaboración de múltiples actores promueve el entendimiento compartido del impacto multifacético de los ataques cibernéticos, y ayuda a construir un consenso respecto de las maneras en que la legislación internacional existente rige el comportamiento de naciones-estado en el internet. Estos cambios reflejarán un constante aprendizaje respecto del ambiente cambiante de las amenazas, y ayudará a promover un acercamiento holístico a la administración del riesgo sobre ciberseguridad. Foros de expertos tales como el de Líderes Europeos de la Industria de la Ciberseguridad, 3GPP SECAM, el Grupo de Trabajo sobre Seguridad y Privacidad en la Economía Digital de la OCDE y el Foro sobre Respuestas a Incidentes y Equipos de Seguridad, son esfuerzos encomiables, que proveen guías detalladas sobre las formas para conceptualizar y entender a los actores de las amenazas, las herramientas y las manifestaciones técnicas. Adicionalmente, los Equipos de Respuesta a Incidentes Computacionales (ERIC) nacionales y regionales pueden actuar como convocantes para los actores, y permitir la educación y mejores prácticas respecto de temas de ciberseguridad.

Una cooperación público-privada efectiva es esencial para fortalecer la seguridad en el internet y responder al amplio y creciente rango de amenazas de ciberseguridad al internet global.

RESPECTO DE LA CÁMARA INTERNACIONAL DE COMERCIO (ICC)

La Cámara Internacional de Comercio (ICC) es la representante institucional de más de 45 millones de compañías, en más de 100 países. La misión principal de la ICC es hacer que los negocios trabajen para todos, todos los días y en todo lugar. Por medio de una mezcla única de promoción, soluciones y establecimiento de estándares, es que promovemos el comercio internacional, una conducta de negocios responsable y un acercamiento global a su regulación, además que proveemos servicios de resolución de controversias líderes en el mercado. Nuestros miembros incluyen muchas de las compañías líderes en el mundo, PYMEs, asociaciones de negocios y cámaras de comercio locales.

INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

33-43 avenue du Président Wilson, 75116 Paris, France
T +33 (0)1 49 53 28 28 E icc@iccwbo.org
www.iccwbo.org @iccwbo