Relatoría del "Diálogo entre autoridades responsables de la seguridad cibernética de la región mesoamericana" (CEPAL – COMTELCA, 11/09/2020)

El Diálogo entre autoridades se realiza en el marco de la asistencia técnica solicitada a CEPAL por parte de la Dirección de la Comision Técnica Regional de las Telecom (COMTELCA). La CEPAL ha venido trabajando con distintos actores de la región, en la construcción de un diálogo público – privado, dirigido a la construcción de una estrategia - país en materia digital y de seguridad cibernética. Es en este contexto que se enmarca la asistencia técnica a COMTELCA.

Moderador: Allan Ruiz Madrigal, Secretario Ejecutivo COMTELCA

Introducción: Georgina Núnez, Oficial de Asuntos Económicos, CEPAL

El proceso de digitalizacion de las economías de la región de los últimos años, acelerado en la actual coyuntura de pandemia, ha traido consigo el aumento de las amenazas a la seguridad cibernética. Ello ha conducido a los países a la busqueda de una estrategia nacional de ciberseguridad, construida a partir de un diálogo entre distintos actores de la sociedad (públicos y privados), que den a dicha estrategia una gobernanza efectiva. Además de un diálogo entre los actores, se requiere de una coordinación al interior de los gobiernos, a todo nivel (intraregional e interregional), condición fundamental para enfrentar las amenazas a los aparatos del estado, las empresas y la ciudadanía.

Hemos identificado 4 mensajes que queremos transmitir: 1) La seguridad cibernética o digital representa un esfuerzo coordinado a nivel nacional, en momentos de creciente digitalización de las economías y el aumento de las amenazas de ataques al sistema de información de los países ; 2) Se requieren marcos normativos e institucionales eficaces y una política pública con lineamientos claros sobre la protección de datos (personales y de empresas), que acompañe una estrategia nacional para enfrentar los nuevos desafíos que plantea la digitalización. 3) Dado que el tema se enmarca en un contexto global, la cooperación y esfuerzo multilateral es clave para enfrentar las amenazas cibernéticas. Y por último, 4) la construcción de una estrategia en ciberseguridad amplia y efectiva, requiere de alianzas entre los distintos sectores público y privado.

Una estrategia de seguridad digital debe contar con un esquema de gobernanza efectiva construida con: marcos normativos e intitucionales, mecanismos de respuesta efectivos, desarrollo y protección de infraestructura y sistemas críticos de datos, mecanismos de **c**ooperación internacional para formar un marco multilateral, y por último, una gestión de capacidades y tecnología para enfrentar los diferentes desafíos. Es necesaria una agenda holística que incluya las distintas dimensiones de la seguridad de datos. Esto es, desde la perspectiva de la defensa; la seguridad nacional; la economía, la salud, el orden público, y la política.

Por qué son importantes los marcos normativos e institucionales? El aumento de los ataques cibernéticos ha incrementado los riesgos asociados a la reputación de las empresas en el mundo, Los ciberataques tienen objetivos claramente identificados, no obstante es dificil adelantarse a ellos. Los ataques a la seguridad digital representan costos para las personas, gobiernos, empresas, así como para los sistemas de información en general. El tratamiento de los programas informáticos maliciosos (malware, spyware, data breaches y ransomware) el robo de datos

sensibles, la manipulación de datos, obstaculizar el funcionamiento de sistemas informáticos son tan solo algunas de las amenazas que enfrentan las economías y sociedades de la region[1]

Cuando se habla de marcos normativos de amplia cobertura, un tema clave es la protección de la infraestructura crítica de los países, ausente en la mayoría de los marcos legales de ciberseguridad vigentes en la región. La amenaza o ataques a la infraestructura afecta a sectores clave como: servicios públicos, alimentos, combustible, transporte, comunicaciones, finanzas. Con impactos sobre la sociedad, ya que puede agotar los fondos del tesoro público, atentar contra el suministro del servicios básicos, la red eléctrica, las telecomunicaciones y en el marco de la actual crisis sanitaria.

La capacidad de respuesta de los países a los ataques dependerá en gran medida, del tamaño, diversidad y dinamismo de las estructuras económico – sociales de los países, elementos clave para responder a los ataques cibernéticos y atender sus efectos. Particularmente, los impactos sobre las instituciones, ya que ello merma la fortaleza de la gobernanza ante la exposición a distintos tipos de riesgos, a las estructuras gubernamentales (federal, nacional, regional, estatal, municipal) con consecuencias económicas en ingresos de múltiples flujos (de contribuyentes), en múltiples formas (impuesto a la renta, IVA, etc.) y el nivel de diversificación económica para atender dichos riesgos[2]. Los riesgos para la estructura "política", derivados de un ataque, pueden dirigirse al uso de datos personales para fines políticos obtenidos de manera ilícita: i) en redes sociales para influenciar a votantes; ii) mediante la manipulación de esos datos, a través de amplias plataformas digitales. Riesgos para los sistemas de datos efectivos que protejen a las personas del robo de identidad, y a organismos públicos de posible fraude. Se requiere de personas capacitadas para enfrentar los distintos desafíos y amenazas de manera eficiente.

La dimensión internacional y la necesidad de generar un acuerdo multilateral**,** particularmente en el flujo transfronterizo de datos es una prioridad para la estrategia nacional. La cooperacion multilateral para la protección de datos, y el resguardo de la privacidad, debe garantizar el consentimiento de los propietarios de esos datos, cuando estos trascienden fronteras. Asociado a esta dimensión es importante mencionar, el papel del marco dado por el Convenio de Budapest.[3]

Finalmente, una tercera dimensión de creciente importancia a ser incorporada en una estrategia nacional de ciberseguridad, el llamado monopolio de datos o "data-opolies", que en los tiempos actuales de pandemia, representa una de las principales amenazas a la seguridad digital. Esta

[1] Según el WEF se estima que para el 2021 el impacto económico de los incidentes de ciberseguridad podria alcanzar los $ 6 billones a nivel global. Tan solo en el mes de mayo, al comienzo de la pandemia, Google reportó 18 millones de maleware y fishing mails; y 240 millones de mensajes spam. El Reciente ataque (ransomware al BancoEstado de Chile que representó el pago de casi 9 millones de dólares para recuperar el control de sus plataformas y datos

[2] Por ejemplo, un informe de PWC (2019) para la Comisión Europea señala que el robo relacionado con la seguridad digital de los secretos comerciales en Europa en 2018 significó perdidas por 60 mil millones de euros para el crecimiento económico y casi 289 000 puestos de trabajo. Las estimaciones que este mismo informe hace para 2025 hablan de un impacto de un millón de puestos de trabajo perdidos.

[3] El Convenio de Budapest en su articulo 32.b define el acceso a datos transfronterizos y dice que: El acceso a datos transfronterizos es una excepción al principio de territorialidad que permite el acceso transfronterizo unilateral sin necesidad de asistencia mutua en situaciones limitadas por: i) que los datos sean accesibles al público (fuente abierta); y ii) que una de las Parte haya accedido o recibido datos de fuera del territorio, a través de un sistema informático, con consentimiento legal y voluntario de la persona, con autoridad legal para revelar los datos a través de ese sistema.

dimensión requiere de la coordinación de instancias distintas de gobierno para limitar el poder de los monopolios de datos, a nivel de toda la economía. Lo que incluye: 1) limitar la concentración, no solo de las grandes empresas tech y propietarios de las principales plataformas, sino también empresas de la economía real, cuyo valor ha aumentado sustancialmente, debido al acceso a mayor cantidad de datos. Los efectos de red, la falta de portabilidad de datos, los derechos de los usuario sobre sus datos y la débil protección de la privacidad, ayudan a los monopolios a mantener un dominio. La mayor concentración de datos se convierte es un importante incentivo para los ataques cibernéticos masivos. 2) Sin duda una mayor coordinación entre los encargados de hacer cumplir las leyes antimonopolio y los funcionarios de protección de la privacidad y del consumidor, aumenta las garantías de condiciones para una competencia y privacidad efectiva y que, al mismo tiempo, no se convierta en un impedimiento a la innovación.

Algunas recomendaciones:

- En la región, el tema de la ciberseguridad se asocia fundamentalmente a la protección de datos, por lo tanto, el fortalecimiento de una política en esa dirección debe incluir necesariamente la seguridad digital.
- En la discusión actual, el poder de los datos y su valor creciente demanda una mayor protección ante múltiples ataques. Este es un tema central en las iniciativas internacionales las cuales, entre otras cosas, busca que el usuario que accede a cualquier plataforma pueda proporcionar y controlar su información y que esta quede debidamente cautelada.
- La colaboración público – privada es fundamental en el éxito de una política de ciberseguridad efectiva, en la detección de riesgos asociados al uso y mal uso de datos personales, en la mitigación de los daños que un ataque cibernético pueda producir a la infraestructura crítica.
- Un esfuerzo multilateral requiere de marcos amplios que contemplen las formas y grados variados del impacto de los ciberataques sobre las empresas, gobiernos y sistemas de información. Desde posibles daños a la infraestructura crítica de un país, los alcances de los programas maliciosos y un marco para el flujo transfronterizo de datos.
- Una estrategia regional en ciberseguridad tiene un doble efecto: que las personas tomen conciencia sobre el valor de sus datos y los protejan; y que los reguladores puedan dimensionar con mayor precisión los alcances de un ecosistema digital, elemento esencial en términos de valor, riesgos y rentabilidad.

Héctor Lehuedé, Consultor

El reporte “La ciberseguridad y el rol del directorio en Latinoamérica y el Caribe”, publicado por CEPAL y que hoy presentamos[4], analiza la situación de la ciberseguridad en su relación con el sector privado y el rol de los directorios que velan porque las empresas adopten estándares de ciberseguridad adecuados, para proteger todos sus activos intangibles vinculados a datos. El sector privado tiene un rol importante que cumplir, de la mano del sector público. El aumento de flujos digitales, desde que comenzó la pandemia, han hecho que este tema adquiera relevancia. Es un tema de estrategia empresarial, incorporado en el modelo de negocio de las empresas.

Dada la importancia del tema, se requiere del involucramiento del liderazgo de las empresas para que, a través de la ciberseguridad se protejan, los datos de clientes, usuarios, trabajadores, y proveedores, alrededor del mundo. Se han adoptando estándares, regulaciones, que van

[4] El enlance al document es https://repositorio.cepal.org/bitstream/handle/11362/45988/4/S2000552_en.pdf

generando expectativas para el comportamiento del liderazgo de las empresas en relación a ciberseguridad.

Dentro de un concepto amplio de ciberseguridad existe tres subgrupos: i) el grupo de la ciberseguridad corporativa, se encarga de la prevención de ciberataques y la construcción de seguridad para proteger sus sistemas de TIC y los datos del robo y fraude de sus clientes y consumidores ; ii) el que se preocupa del cibercrimen, de la persecución de delincuentes en la web; y iii) el del ámbito de la ciberdefensa que puede ser, militar o civil, se ocupa de defender los intereses nacionales o atacar al enemigo en el ciberespacio. De la investigación se desprende que, dos de estas tres áreas tienen expectativas concretas respect a lo que las empresas deben hacer.

La ciberseguridad afecta a la propiedad de las empresas, a sus accionistas, pero sigue en el ámbito privado. Distinto es cuando se roban datos personales y sensibles de los usuarios y ciudadanos. En ese caso actúa la regulación recordando a la empresa, el interés de proteger los datos. Desde un enfoque basado en el daño que esto puede causar (multas, responsabilidad corporativa y daño reputacional). Es un enfoque legal, sancionatorio, de protección de datos.

Desde la ciberdefensa a civiles está la protección de la infraestructura y los servicios críticos. En este caso, el enfoque no está tanto en la responsabilidad o las multas, sino que en las organizaciones, y las medidas necesarias que deben adoptar para evitar los eventos de ruptura del servicio, o si se producen uno de estos eventos la recuperación sea lo más rápido posible. Este enfoque es más técnico que legal, y mucho más operacional, enfocado principalmente en las empresas que manejan infraestructura crítica y servicios esenciales.

Las expectativas se han ido traduciendo en políticas, en regulaciones, en algunos casos en recomendaciones, pero cada vez más con un mayor énfasis normativo. Dentro de la región encontramos más regulación orientadas hacia el primer grupo, la protección de datos. No se encontró casi regulación concreta de ciberseguridad para infraestructura crítica y servicios esenciales. Esta es más la práctica de los países con mejores rankings de ciberseguridad.

Los países miembros de COMTELCA presentan estándares adecuados de protección de datos. La regulación o el nivel de protección es adecuado. En su mayoría, dichos países han adoptado una estrategia de ciberseguridad y con ello, la existencia de niveles de respuesta a ciberataques. La infraestructura y servicios críticos son prácticamente inexistentes en estos marcos normativos. Hay ausencia de una adecuada protección a servicios digitales, responsabilidad de los proveedores de servicios digitales por la ciberseguridad, protección de servicios esenciales, identificación de los operadores de servicios esenciales, requerimiento de ciberseguridad para esos operadores y monitoreo regular de la ciberseguridad que ellos hacen. Este es un tema de larga discusión en la región. En 2004, la Asamblea General de la OEA aprobó una estrategia integral para combatir amenazas a la seguridad cibernética y propuso la adopción de estrategias nacionales de ciberseguridad que pudiesen gestionar los riesgos sobre la infraestructura crítica. Además, estos ataques a la infraestructura crítica fueron calificados como el quinto mayor riesgo a nivel mundial por el World Economic Forum.

El estudio arrojó pocos resultados respecto a la incorporacion de la infraestructura crítica en la estrategia nacional de ciberseguridad. La mayoría de los países no han identificado con precisión las infraestructuras que deben considerar críticas o las entidades que las controlan, los estándares de ciberseguridad que necesitan implementar para protegerlas y el monitoreo y responsabilidad que asegurarán que esos estándares se implementen. Algunos casos de estudio, algunas buenas prácticas y estándares de ciberseguridad se incluyen en este informe.

Una recomendación a las empresas y sus directorios es asegurarse de reducir los riesgos hacia estas infraestructuras. Cuando empresas privadas administran activos críticos y servicios esenciales es importante que tengan un nivel de inversión en ciberseguridad acorde con las expectativas de los ciudadanos y del país. Estos servicios deben estar disponibles en casos de emergencia, porque la ciudadanía depende de ellos en su cotidianeidad, así como del teletrabajo y la teleducación, en la actual pandemia.

Uno de los estudios sectoriales, presentado en el documento, se refiere al sector financiero en distintos países. Este ha ido adoptando normas para asegurar que los bancos, agentes importantes en la cadena de pagos, tengan una ciberseguridad adecuada. Recientemente, el Banco Estado de Chile, empresa pública y del sector financiero fue hackeada por un *ransomware* que afectó 13 mil de sus computadores y que, por varios días, impidió abrir sus sucursales, solo se pudo operar en algunos servicios en línea. El Banco Estado es una empresa 100% estatal, por malas reglas de gobierno corporativo no está sometida a las normas de control y supervisión del sistema de empresas públicas de Chile. Es una empresa que tiene 7 miembros en su junta directiva, 6 de los cuales son nombrados por el Presidente de la República, sin ningún proceso de selección professional. La Comisión para el Mercado Financiero, regulador de las empresas listadas y de los bancos en Chile, ha señalado que la visión del regulador es que las mejores prácticas internacionales consideran involucrar al directorio y altos ejecutivos a que asuman responsabilidades claras sobre el manejo de riesgos a la ciberseguridad, de forma tal que las instituciones financieras cuenten con protocolos, roles y equipos especializados y se ejecuten pruebas de tensión y de escenarios . El rol del supervisor en este esquema es velar porque el marco de gestión de riesgo operacional y de ciberseguridad sea implementado y funcione adecuadamente.

Comentaristas:

Ing. Daniel Casados, Secretaría de Economía

La ciberseguridad gira en torno a los datos. Desde una perspectiva de política pública, donde el principal objetivo es el beneficio de la sociedad, el trabajo coordinado por el Estado con el conjunto de la sociedad adquiere gran relevancia.

Dos elementos a destacar de la actual situación de la ciberseguridad: i) no existe una coordinación en los esfuerzos desplegados para enfrentar la ciberseguridad; y ii) la falta de una definición clara del significado de los datos y el no entendimiento sobre lo que implica la ciberseguridad. En este sentido, la pregunta es cuántas instancias existen en nuestra región que tengan la suficiente autoridad para poder modelar y llevar a cabo, tanto la implementación como la ejecución de las políticas públicas que pudieran estar enfocadas en los dos términos mencionados, por un lado los datos y por otro la ciberseguridad.

Revisando la normalización de los datos y la ciberseguridad, se observa que ambas instancias están representadas en distintos órganos, tanto en términos de la jerarquización, como en lo público y lo privado. Dificilmente se encuentra una entidad que tenga la capacidad de gobierno superior para implementar protocolos,etc. Por tanto, se habla de esfuerzos realizados de manera no coordinada, aislada y cuyo principal reto es la capacidad de conectar todos los que require de una necesaria centralidad, capaz de llevar a cabo las distintas actividades. No hay esa autoridad central en la región, por lo que los mayores esfuerzos se diluyen en las mejores prácticas que no necesariamente atiende los problemas o necesidades localizada.

La ciberseguridad se debería establecer a través de politicas públicas que atiendan las necesidades localizadas, pero debido a la naturaleza de estos datos, su forma digitalizada, tiene que trascender a acuerdos internacionales, lo que lo vuelve aún más complicado. Es decir, se puede correr el riesgo de implementar politicas públicas altamente focalizadas que no estén en equilibrio con lo que esta sucediendo en el mundo y que puede ir en detrimento de políticas hacia la ciberseguridad.

Hay un problema en el rol que juegan los datos, la monopolización de los datos. Se trata de un número determinado de empresas en el mundo que tienen acceso a datos personales de manera desequilibrada. Estas empresas pueden tener ciertas influencia en que los datos circulen de manera más libre, usufructuando luego de la extracción de ellos para su propio beneficio. En este punto, la falta de administración y de cobertura hacia la ciudadania en protección de datos tiene un peso importante. Si no se centraliza la administración de los datos, dificilmente se podrá migrar a políticas de ciberseguridad. Por otra parte, si no se centraliza la ciberseguridad, la acción que se tenga ante cualquier ataque cibernético que, por cierto, la administración y las grandes empresas están en constante amenaza, no tendrá el resultado esperado.

Cabe mencionar que, los ataques no son persistentes ni seccionados, tienen distintos tipos de especificaciones. Hay una organización de cibercrimen y estructura criminal que lo que hace es concatenar los distintos tipos de ataque en uno solo. Hay ataques permanentes que no están siendo visualizados ni atendidos de la manera más adecuada. Por otro lado, no hay una conceptualizacion clara sobre los datos. No existe un tratamiento diferenciado de los datos y de la información. La descoordinación que hay del lado de los atacados, no la hay del lado de los atacantes. Existe un desequilibrio importante, debido a que se vuelve un tipo de atención personalizadas y no colectiva para enfrentar los casos. Por lo tanto, la pregunta sería, en manos de quien queda la articulación de esa coletividad que dé la coordinación necesaria como para establecer un frente de defense del tema. Actualmente, la ciberseguridad es un tema reactivo y no proactivo, mientras ocupe ese lugar dificilmente se lograran los acuerdos que se requieren.

Esto no significa que no se estén haciendo los esfuerzos tanto públicos como privados, pero es importante darle lugar prioritario al concepto de ciberseguridad, para que desde arriba se pueda concretar la coordinación de política pública, sobre las responsabilidades que deben existir. Esto, desde luego, implica una inversión importante en términos tecnológicos, y dependiendo de cuál sea la situación se podrá acceder a dichas inversiones para protegerse.

Por último, un tema importante es el de la educación, concientización y sensibilización de los usuarios para entender el acceso al mundo digital. Se requiere elaborar programas para sensibilizar a los usuarios, en cuanto a mitigar los riesgos a los que están expuestos ante un ataque. La mayor parte de los ataques proviene de acciones humanas a nivel de política pública.

Martín Portillo, Huawei, "Caso aplicado de una estrategia de ciberseguridad en empresas.

Huawei es una compañía que tiene presencia a nivel mundial en 170 países, actualmente contribuyen con cerca de 1500 redes a nivel mundial. Redes de todo tipo, inalámbricas, alámbricas, redes TIC, ello nos ha abierto la oportunidad de contribuir con 3 mil millones de personas en el mundo entero, que de alguna manera han utilizado la tecnología de Huawei. Como compañía de tecnología, acumula más de 270 certificaciones de productos con estándares de seguridad internacionales. De igual manera, en la parte de gestión de plataformas, de redes, todo eso es apalancado con la presencia internacional de 14 laboratorios, 14 centros de investigación ubicados en diferentes partes del mundo (Europa, Asia, América y pronto en algunos países de la region). Para Huawei los temas de ciberseguridad no son nuevos, han trabajado en los esquemas

de seguridad, prácticamente desde 1999. Es hasta 2010 cuando establecieron el comité internacional de ciberseguridad y cuya casa matriz está en China.

La aparición de las nuevas tecnologías que hoy estamos implementando a nivel mundial, se expresa en un esquema simple que muestra como la aparición de nuevas tecnologías y nuevos servicios incrementan la complejidad en el manejo de una red de telecomunicaciones tradicional. Normalmente, seguimos los esquemas y estándares de seguridad para redes 3G, 4G o redes alámbricas; la aparición de redes de nueva generación como la 5G nos presentan desafíos muy importantes en el manejo de la seguridad. No solo se trata de cuidar los nichos tradicionales de ataques o vulnerabilidades, ahora hay que segmentarlos también a nivel servicios, plataformas y regiones geográficas. Se deben cuidar los ataques a lo que llamamos RAN (Radio Access Network), que implica todas las etapas de inicio de una transacción digital, de un usuario o servicio que está buscando una comunicación a internet, o simplemente está buscando una comunicación con alguien no necesariamente nativo de esta red, y que quiere alcanzar, probablemente en otra región, país u continente, una comunicación. También enfrentan amenazas a nivel *routers*, amenazas propias del cambio de operación y mantenimiento en redes de telecomunicaciones.

La complejidad lleva a tener respuestas notablemente lentas en ataques, eventualidades, vulnerabilidades, derivadas de la participación de muchos elementos, tantos de redes, servicios y tecnologías diferentes. Con la aparición de nuevas tecnologías, con el uso globalizado de las redes digitales, con las conexiones innumerables que presenta el IoT, etc. hace extremadamente compleja la situación y justifica un desarrollo continuo en el ámbito de seguridad y los estándares de ciberseguridad en redes de alta tecnología.

Hay un involucramiento del *top management* de la organización, responsible de armar la estrategia, planificación, políticas e incluso estrategias de implementación de algunos protocolos y algunos algoritmos dependiendo del país donde operamos. Además de tener una estrategia a nivel corporativo, cada país tiene un representante que es responsable de la implementación de la estrategia global corporativa de ciberseguridad y es también responsable de atender las necesidades locales de las economías, del cumplimiento de las legislaciones vigentes que en ese momento se encuentra en el país así como los acuerdos con los clientes propios de este país.

Huawei tiene a cerca de 2 mil profesionales a nivel mundial dedicados exclusivamente al seguimiento e implementación de la estrategia de ciberseguridad. Algunos de ellos concentrados en los 14 laboratorios donde realizan I&D, hacen pruebas y verifican que los estándares de seguridad y protección de datos se implementen de manera adecuada, conforme a los estándares internacionales que deben cumplir. Han adoptado los procesos CERT, certificación que se expide en EE.UU., adoptada en muchos países. A finales de 2016 lanzaron la Agencia Central de Cuidados de Ciberseguridad a nivel global. A partir de 2018, el tema de ciberseguridad ha pasado a ser la primera prioridad dentro de la visión y estrategia de la compañía. Se trata del factor más relevante de los acuerdos comerciales o del desarrollo de algunas tecnologías y la aplicación de los estándares adecuados para mantener la ciberseguridad en las redes.

Se enfocan en el cuidado de la seguridad desde 12 áreas de productos y servicios. Aplican la estrategia y la gobernanza definida desde el corporativo, las cuales hacen coincidir con las estrategias locales de cada país. Adoptan los estándares internacionales pertinentes dependiendo del segmento que se trate. Se certifican con la entidad correspondiente, para garantizar que los productos y servicios cumplan con esa normatividad. Se aplica la norma técnica, dependiendo de los requerimientos de cada economía o aplicación en cuestión. Además existe un código de comportamiento de conducta de los empleados, para hacer cumplir los lineamientos de ciberseguridad demandados por la legislación de cada país donde tienen presencia. Inclusive, las

personas que trabajan en los esquemas de seguridad de la empresa firman contratos diferentes, donde se garantiza el cumplimiento de todos los lineamientos de conducta y de aplicación de normas para todos los procesos de ciberseguridad.

El 5% de los recursos anuales destinados a I&D de tecnología están destinados a investigaciones en temas de ciberseguridad. Actualmente cuentan con un fondo de 2 mil millones de dólares para la investigación en temas de software y aplicaciones para esquemas de ciberseguridad. También cuentan con procesos de auditoría, con procesos de trazabilidad. Producen 5 mil millones de códigos de barra por año que les permite identificar, de forma rápida, algún bloqueo, dispositivo, código sospechoso de algún ataque o vulnerabilidad y reaccionar de forma inmediata y atender el problema.

La parte de *delivery* de manufactura son bloques que siguen los estándares internacionales, siguiento la ISO 28.000, el T-PAT, TAPA entre otros. Por ultimo, en cuanto a la filosofía de verificación llamada ABC (*Assume nothing, Believe no one, Check everything)* que significa "no suponemos nada, no le creemos a nadie y chequeamos todo", independientemente de la información o del origen del producto se hace una triple verificación de insumos y procesos para la entrega final de insumos de un cliente especifico. Sobre estos insumos, actualmente tienen acuerdos con prácticamente cuatro proveedores de insumos. Para ser parte de la Plataforma de la empresa, se certifica la homologación y la certificados en un proceso de seguridad.

Al recibir una solicitud de producto o servicio de algún cliente, operador o entidad gubernamental, se cuida que estos requerimientos ya tengan incluidos los estándares de seguridad que esperan tener, como primera validación. Se busca que desde el inicio, los servicios y productos ya tengan una certificación clara en términos de ciber resiliencia o ciberseguridad. La parte de diseño, la parte legal y la manufactura e instalación siguen prácticamente estándares y protocolos internacionales que son auditables. Cada proceso, o segmento de negocio está perfectamente identificado con un estándar internacional, auditable, comprobable y verificable, incluso en los propios laboratorios de la compañía que ponen a disposición de sus cliente y socios tecnológicos.

Respecto a las buenas practicas, el referente europeo para la protección y regulación de datos es el GDPR, el cual es muy útil para las economías que todavía no tienen una legislación probada en protección de datos. Otra buena práctica tiene que ver con la aparición de 5G, se trata de un programa definido por 3GPP y GMSA, denominado NESAS. Su objetivo es garantizar dos cosas: 1) garantizar que el fabricante del equipo cumpla con estándares de seguridad, calidad de la seguridad; 2) dar la oportunidad de evaluar que el equipo que produce este proveedor de tecnología cumpla con esos estándares. Es importante para los países de la region donde ya se esta desplegando la tecnología tipo 5G, como un buen referente a considerar para temas de estándares, calidad y selección de tecnología.

Se resaltó el caso de Alemania, que comenzó los estudios de ciberseguridad hace alrededor de 20 años. Desde 2001 son parte del ENISA; en 2005, como primer país europeo, publicó su plan de protección de infraestructura; en 2016 publicó su estrategia de 9 objetivos de ciberseguridad. Finalmente, en octubre de 2019, la entidad reguladora de telecomunicaciones de Alemania publicó y compartió su catálogo de requerimientos de seguridad para la operación de sistemas de telecomunicaciones y procesamiento de datos. De esta se desprendieron 10 criterios utilizados para evaluar o requerir el nivel de seguridad a cualquier proveedor o usuario de tecnología.

Areli Zarahi Rojas, **Sec. Técnica de la Mesa de Construcción de Paz y Seguridad del Estado de Tlaxcala (AMEXID)**

A pesar de los avances, en la región hay todavía un largo camino que recorrer. Si nos comparamos con el resto del mundo, en Europa existe una directiva NIS que justamente regula todos los procesos, reglas y estándares de tecnología, importante para las infraestructuras criticas del sector público y privado. Ello ha beneficiado a los países europeos, frente a los múltiples ataques cibernéticos y la vulnerabilidad de datos. Esta directiva homologa los procesos de toda la región, lo cual resultó muy beneficioso para la seguridad de los datos, lo cual es un gran reto.

Actualmente los países tienen que hacer una ciberdefensa para poder actuar como Estados-Nación y la región no es la excepción. Por ejemplo, en 1994 en México, se presentaron los primeros intentos de hackeo. Antes los hackers lo hacían por diversión, entraban a las páginas de gobierno y ponían algún letrero del Ejército Libertador Zapatista y esos eran los ataques. Pero ahora ponen en jaque a las infraestructuras críticas, incluyendo las de gobierno. Afortunadamente, en México no se ha llegado a una escala en que se tenga que proteger la infraestructura critica como se ha visto afectada físicamente en varios casos. No solo el malware inyectado, sino que ha llegado a paralizar la infraestructura de forma física y los países de la región somos vulnerables frente a eso, ya que si nos llegan a paralizar la producción petrolera o la luz estaríamos en graves problemas.

Es también un tema de seguridad nacional, de igual forma que es el centro financiero, donde se ven los mayores avances en México y en la region. En este sector sobre todo los bancos se cuenta con los llamados CISO (Chief Information Security Officer), jefes de seguridad de las empresas que manejan grandes datos, Huawei no es la excepción.

El sector académico también está incursionando no solo en hacer propuestas legislativas y de políticas públicas, sino en tener el equivalente a los CISO dentro de sus universidades, para proteger su propia infraestructura crítica para hacer investigación.

Tenemos que implementar buenas prácticas, que hay que formalizer e institucionalizar, a través de un ente rector. Se deben hacer las reformas necesarias a la legislación porque ahí es donde todavía falta mucho. Ojalá que, a través de los mecanismos existentes en la region, se pueda impulsar una normativa similar a la NIS. A pesar de que la organización de la región es distinta a la de la UE, es possible hacer esfuerzos para que de los organismos pueda surgir una directiva consensuada entre los países que puedan, cada uno de ellos, ir adoptando en su legislación y política pública e implementando las directrices de ciberseguridad, protección de datos y de ciberseguridad educativaya que desde ahí se empieza. Hoy está abierta la participación en la UE para reformar la iniciativa NIS, debido a que deja un poco fuera el internet de las cosas. Actualmente, todo está conectado con el internet de las cosas y es a través de los aparatos que aumenta la vulnerabilidad, tanto en tema de datos como en intrusiones digitales.

En México hay un área científica de guardia nacional, cuyo sistema previene y ataca acciones maliciosas, que pueden llegar a México, sobre todo a instituciones de gobierno, cuentan con herramientas de ciberseguridad e inteligencia impactantes. La Secretaría de Marina, de Defensa Nacional, la Fiscalía General y cada uno de los 32 estados de la República tienen, en mayor o menor medida, herramientas similares, lo que se dificulta es la fusion de todos estos recursos existentes para conformar un solo frente. Esta situacion puede estar sucediendo algo similar en la mayoría de los países de la region, pese a los avances de países como Chile, Argentina y Brasil, todavía falta una directiva que impulse a los países.

Luis Alberto Martínez Bibiano, Director de Gestión de Seguridad de la Información de la Secretaría de Marina de México

La Secretaría de Marina tiene dos roles fundamentales: una como fuerza armada y la otra el rol fundamental como Secretaría de Estado. Como fuerza armada, desde 2004 ha estado desarrollando capacidades de seguridad de la información, ciberseguridad y ciberdefensa, conforme evolucionan estos conceptos) y enfrentando las ciber amenazas. Sobre este punto se han desarrollado varios proyectos. Desde hace dos sexenios, se ha considerado el programa sectorial de marina en ciberseguridad, como actor fundamental para la seguridad nacional. Como Secretaría de Estado se cumplen dos funciones; una como autoridad marítima nacional, donde lidera el proyecto de gestión de riesgo cibernético marítimo, y están obligados a cumplir en 2021 las directivas que emite la Organización Marítima Mundial de la ONU. El mayor esfuerzo se enfoca en brindar esa seguridad cibernética a todo el sector marítimo. El otro esfuerzo es como instancia de seguridad nacional, participando en el Consejo de Seguridad Nacional, en donde el consejo tiene varios comités especializados. Dentro de ellos, está el comité especializado de seguridad de la información, el cual está conformado por las 11 dependencias que conforman el bloque de seguridad nacional: Hacienda y Crédito Público, Función Pública, Relaciones Exteriores, Gobernación, Fiscalía General de la República, Secretaria de Protección y Seguridad Ciudadana, Defensa Nacional y Secretaría de Marina.

En el comité especializado existen dos grupos técnicos, el Grupo Técnico de Seguridad de la Información, donde lidera la Secretaría de Marina, y el Grupo Técnico de Armonización Legislativa en donde se han hecho enormes esfuerzos, desde 2010, en la generación de normatividad para el tema. Uno de los principales logros que ha tenido ambos grupos es la publicación del Manual Administrativo de Aplicación General de Tecnologías de la Información y Seguridad de la Información, documento que obliga a todas las dependencias de gobierno a gestionar los riesgos de seguridad de la información.

El reto es cómo lograr la implementación de la seguridad de la información en las dependencias, como parte preventiva fundamental para enfrentar los retos que presenta el ciberespacio. Juegan un rol fundamental las economías de la protección ciudadana, donde a través del CMX se ha activado, desde hace más de 5 años, el protocolo de protección a infraestructuras críticas a nivel nacional y se ha apoyado y atendido los ciberataques que recibió PEMEX (Petróleos Mexicanos), en este caso se ha colaborado con el CMX, ente rector en materia de protección de seguridad ciudadana y se ha llevado a cabo el enfoque de la seguridad nacional a la protección de las infraestructuras críticas.

Coincidió con Casados de que se requiere de un ente rector, cada dependencia va haciendo su mejor esfuerzo. Es muy importante buscar el tema de la gobernanza del ciberespacio desde un enfoque multidimensional como el que se analiza en este diálogo. Han sido muy buenos los aportes que se han hecho y en ese sentido. La Secretaria de Marina propuso, en primera instancia, tener un repositorio donde compartir la legislación en materia de protección de datos personales y normatividad (como el MATICSIC o manual administrativo) de los países de la región, de manera que se vaya socializando el tema e impulsando la legislación que se necesita.
En México la Secretaria ha participado en asesoría a algunas iniciativas de ley. Pero la legislación va un paso atrás de las ciber amenazas, a pesar de los esfuerzos desplegados. Se requiere de mayor concientización, al más alto nivel, de todos los organismos y dependencias de gobierno. Dado el presente reto del ciberespacio y donde el desarrollo tecnológico es increíble, que va más delante de nuestras propias capacidades. La cooperación es el factor fundamental en este tema. Eventos como este permite la socialización y difusión de la información y de los esfuerzos de cada país.

María Eugenia Hernández, Diputada Federal y Secretaria de la Comisión de Ciencia, Tecnología e Innovación. Cámara de Diputados (as) de México

Desde la Comisión de Ciencia, Tecnología e Innovación, se lleva la agenda legislativa del tema de la ciberseguridad. Se ha avanzado en un punto de acuerdo que se inclyó el 29 de octubre de 2019, en relación a la solicitud de adhesión de México al Convenio de Budapest, considerado uno de los primeros pasos que se tenía que dar. El 8 de enero de 2020 se puso a consideración una iniciativa sobre amenazas a la seguridad nacional, los actos ilícitos perpetuados en el ciberespacio, que se adiciona en los artículos quinto y sexto de la ley de Seguridad Nacional. También se realizó un punto de acuerdo que exhorta al Ejecutivo Federal, la Secretaría de Gobernación, y a la Secretaría de Protección Ciudadana para que se realice un diagnóstico sobre la Estrategia Nacional de Ciberseguridad en México.

El 9 de julio de 2019, la Comisión de Ciencia, Tecnología e Innovación realizó el foro sobre Ciberseguridad y Desafíos Actuales y Futuros en México. El pasado 12 de agosto se propuso una iniciativa para declarar el 23 de noviembre día nacional de la ciberseguridad.
Como se puede ver desde la propia Cámara de Diputados hay mucho interés en el tema de la ciberseguridad nacional. Se sabe que diversos legisladores hay un compromiso para que en sus legislaturas sean cubiertos estos temas.

Un desafío para México, es hacer entender al ciudadano común la importancia de la ciberseguridad. Como legisladores y en la propia comisión se ve la necesidad de sumar esfuerzos. Se reconoce que se está realizando un trabajo sobre el tema, pero son esfuerzos aislados. Si como legislativo se lograra sumar esfuerzos, el tema podría avanzar en forma más acelerada,

En México estamos viviendo un problema muy fuerte en seguridad, creemos que la ciberseguridad podría ayudar a resguardar los temas que la propia ciberseguridad plantea. Consideramos que el avance tecnológico puede permitir la seguridad a nivel nacional. Hay que adecuarse al desarrollo tecnológico. Para ello, se han realizado mesas de trabajo, foros, conversatorios, y actualmente se tiene programada la celebración de un foro a nivel latinoamericano sobre el tema de ciberseguridad, cuyo diseño estará listo la primera quincena de octubre, y al que todos ustedes estarán invitados. Se han aglutinado diversos sectores de todo el ecosistema tanto a nivel federal, legisladores, y de la iniciativa privada, para tratar de conjuntar la suma de voluntades. La agenda de la ciberseguridad se ha sumado ya a la agenda legislativa de la Comisión de Ciencia, Tecnología e Innovación.