Introducción a la Gobernanza de Internet en LAC

Módulo 5.1: Ciberseguridad.

Definir qué se entiende por ciberseguridad, es una tarea compleja, ya que no existe una definición uniforme y universalmente aceptada. Sin embargo, existen dos definiciones que podemos tomar como punto de partida para analizar el tema de la ciberseguridad desde la perspectiva de la gobernanza de Internet.

La primera definición, es la provista por la **National Initiative for Cyber Security Careers and Studies (NICCS)**, que establece: La ciberseguridad es la actividad o proceso, habilidad o capacidad o estado por el cual los sistemas de información y comunicaciones y la información contenida en ellos están protegidos y/o defendidos contra daños, uso o modificación no autorizados o explotación.

La segunda definición provista, es la que se encuentra incluida en la Recomendación UIT-T X.12057 sobre los aspectos generales de la ciberseguridad, emitida por el Sector de Normalización de las Telecomunicaciones de la Unión Internacional de las Telecomunicaciones (la UIT-T).

Se complementa lo anterior con la definición que en dicha Recomendación se brinda al ciber entorno, incluyendo a usuarios, redes, dispositivos, todo el software, procesos, información almacenada o que circula, aplicaciones, servicios y sistemas que están conectados directa o indirectamente a las redes.

A los fines del presente análisis, se utilizarán las definiciones mencionadas y centradas en los aspectos defensivos de la ciberseguridad, sin desconocer la existencia de otro inmenso enfoque –estrategias ofensivas de ciberseguridad.

Uno de los primeros obstáculos que hay que sortear, es la confusión con otros conceptos que pueden aparecer como similares. Como lo expresó Alexander Klimburg en 2017 lo anterior sucede con conceptos como seguridad de la información y seguridad informática, con lo cual se confunde a los usuarios y a los expertos en seguridad y no permite ver las diferencias críticas entre ambas disciplinas. Asimismo, sostiene Klimburg, que la ciberseguridad comprende un amplio rango de prácticas, herramientas y conceptos estrechamente relacionados con los de seguridad informática y operacional, donde la ciberseguridad se distingue por su inclusión del uso ofensivo de las tecnologías de la información para atacar a los adversarios. Es

decir, dicho autor incluye dentro del ámbito de la ciberseguridad a la dimensión referida a una estrategia ofensiva de la ciberseguridad.

Si bien el foco del módulo se encuentra asociado a la ciberseguridad, la misma se encuentra en la práctica relacionada con la **ciberdefensa** y los **ciberdelitos**.

La ciberdefensa puede ser definida como el conjunto de medidas técnicas y no técnicas que permiten a un Estado defender en el ciberespacio los sistemas de información considerados esenciales. Esta definición proviene de un documento elaborado por una comisión especializada para la Asamblea Nacional de Francia en 2018 con el objetivo de precisar todos los conceptos relacionados con la seguridad en el ciberespacio.

El cibercrimen se compone de actos que contravienen los tratados internacionales o las leyes nacionales, utilizan redes o sistemas de información como medio para cometer un delito, o atacarlos, de acuerdo con la definición elaborada por el Convenio de Budapest en 2001. Este convenio promovido por el Consejo De Europa ha sido ratificado por Europa y adoptado por varias naciones del norte, Asia y también de América Latina (como Argentina, Chile, Colombia, Costa Rica, Panamá, Paraguay, República Dominicana).

Ambos, **ciberdefensa y ciberdelitos,** tienen como actor fundamental al Estado, pero fundamentalmente en el contexto de las definiciones de lo que es infraestructura crítica y la organización y gestión de los centros de respuesta a incidentes informáticos, estos temas se tornan mucho más complejos por la variedad y diversidad de actores, incluyendo al sector privado, que entran en juego como señalan autores como Bradshaw (en 2015), Hurel y Lobato (en 2018) y Bustos y Aguerre (en 2020).

De esta manera, la ciberseguridad es un abordaje mucho más amplio que la ciberdefensa y el cibercrimen, aunque en muchos aspectos los incluye y por ende el campo de acción de los tres tiene algunos puntos de contacto.

Volviendo a enfocarnos sobre la ciberseguridad y el papel de las múltiples partes interesadas, Vishik, Matsubara y Plonk citando al libro blanco adoptado por diferentes asociaciones de la industria en Europa, Asia y Estados Unidos referido a las recomendaciones de la industria y el gobierno para continuar con el crecimiento y la seguridad en el ciberespacio, refieren que todos los stakeholders (o sea gobiernos, industria, academia y sociedad civil) deberían trabajar de manera conjunta para

asegurar que los beneficios del ciberespacio sean accesibles para los ciudadanos y que se aborden los principales desafíos.

Para lograr lo anterior, es necesario entonces que los diferentes stakeholders participen, de manera conjunta y en un pie de igualdad, en la elaboración de los principios que deberían informar a las políticas referidas a la ciberseguridad. Es decir, la participación de los diferentes actores interesados debería realizarse en esta primera capa, que permita determinar cuáles son para ellos, los principios de las políticas que se deban respetar en materia de ciberseguridad.

La elaboración de estos principios podrá realizarse a nivel global o si por el consenso de dichos stakeholders resultara más conveniente, más enfocado y más apropiado debido a los diversos escenarios que se puedan aplicar, a nivel regional o local.

Existen diversas fuentes de principios y normas para informar políticas de ciberseguridad. Una de estas fuentes con influencia internacional que retomamos en este módulo proviene de la la Organización para la Cooperación y el Desarrollo Económicos (OCDE), organismo de cooperación internacional compuesto por 36 estados, cuyo objetivo es coordinar sus políticas económicas y sociales. También se ha enfocado en temas de ciberseguridad y desarrollo del ecosistema digital. De nuestra región son miembros Chile y México; Colombia y Costa Rica están entre los países candidatos a adherirse a esta organización.

En las Directrices de la OCDE para la seguridad de sistemas y redes de información: hacia una cultura de seguridad, se enumeran los principios aplicables a la seguridad de sistemas y redes de información, siendo los siguientes: **Concienciación; Responsabilidad; Respuesta; Ética; Democracia; Evaluación del riesgo; Diseño e implementación de la seguridad; Gestión de la Seguridad; y Reevaluación**.

También es importante considerar los principios de ciberseguridad que se encuentran enumerados en la Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro emitido en la Comunicación Conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, del año 2013, donde se mencionan los siguientes: **Los valores esenciales de la Unión Europea lo son tanto en el mundo físico como en el digital; Protección de los derechos fundamentales, la libertad de expresión, los datos personales y la intimidad; Acceso para todos; Gobernanza multilateral democrática y eficaz; y garantizar la seguridad**. Estos principios, adaptados, también deberían poder aplicarse para elaborar una lista de prácticas que informen a las políticas de ciberseguridad, con la participación de los diferentes stakeholders.

Adicionalmente, **Fátima Cambronero** en la publicación **"Ciberseguridad y la gobernanza multistakeholder"** considera que también deberían ser objeto de análisis los principios de diseño o de la arquitectura de Internet, que permitan extrapolar para aplicarse a la ciberseguridad, entre ellos, el de apertura, descentralización, extremo a extremo, mejor esfuerzo, modelo de capas e innovación sin pedir permiso, ya que los mismos son parte de la esencia de Internet; asimismo en dicha publicación recomienda que analizar dichos principios desde la perspectiva de la ciberseguridad, podría brindarle a ésta última, ciertas condiciones de permanencia en el diseño de estrategias que se generen respecto de la misma.

Finalmente, la autora considera que una vez definidos estos principios de las políticas de ciberseguridad, con la participación de gobiernos, sociedad civil, sector privado y comunidad técnica y académica, se debería trabajar en elaborar las normas, estándares y buenas prácticas que resulten aplicables a los diferentes escenarios que se encuentran transversalizados por la problemática que implica la ciberseguridad.

Habiendo establecido, con la participación de los múltiples actores interesados, los principios que deben informar las políticas de ciberseguridad, y habiendo determinado un primer grado de madurez en la comunidad local, es posible comenzar a diseñar una estrategia nacional de ciberseguridad.

Para ello, y reconociendo que no existen recetas universalmente aceptadas y probadas en su eficacia que puedan funcionar en todas las comunidades, se han elaborado y publicado diferentes guías que pueden resultar útiles para estos fines.

El trabajo de **Global Partner Digital**, considera las características que debe tener un enfoque multistakeholder, en la elaboración de estrategias nacionales de ciberseguridad y enumera entre ellas, a las siguientes:

- Debe ser abierto y accesible,
- debe incluir los puntos de vista de las diferentes partes interesadas,
- debe estar basado en el consenso
- y ser transparente y con rendición de cuentas.

Mientras más abierto sea este proceso, se va a facilitar un diálogo más informado que permita que los actores interesados contribuyan con sus puntos de vista y experiencia. Este diálogo, asimismo, ayuda a generar confianza entre las partes interesadas, lo cual es un requisito previo clave para la colaboración y la toma de decisiones por consenso. Adicionalmente, un compromiso con la transparencia y la

rendición de cuentas genera confianza en el proceso de desarrollo de la estrategia y en el resultado final y en su implementación.

Asimismo, el referido reporte de Global Partner Digital define las etapas en el proceso de desarrollo de una estrategia nacional de ciberseguridad, el cual se sugiere complementar con lo establecido en el Framework for multistakeholder cyber policy development, también elaborado por Global Partner.

Se considera importante también incluir en el proceso de desarrollo tanto de políticas de ciberseguridad como de la estrategia nacional de ciberseguridad, las características que establece **Internet Society** para lo que llama seguridad colaborativa, debiendo respetarse los siguientes principios:

- Fomentar la confianza y proteger las oportunidades;
- Responsabilidad colectiva;
- Propiedades y valores fundamentales;
- Evolución y consenso;
- y piensa globalmente, actúa localmente.

Es importante destacar el rol de los gobiernos a la hora de implementar una estrategia de cyberseguridad, ya que es el único actor con capacidad de generar políticas públicas permanentes y con continuidad entre gobiernos.

Módulo 5.2: Ciberseguridad. Funcionamiento y estrategias.

Abordaremos aspectos de funcionamiento de la ciberseguridad así como algunas estrategias específicas desarrolladas por actores internacionales.

Los equipos de respuesta a incidentes de seguridad informática (ó CSIRT por su acrónimo en inglés) son actores clave en el complejo régimen cibernético que se ocupan de prevenir y responder a los incidentes cibernéticos a través del análisis y la respuesta a los incidentes, el intercambio y la difusión de información y la capacitación. Existe consenso entre los miembros y actores de los CSIRTs que hay margen de fortalecer la cooperación a partir de un intercambio mejorado y oportuno de información sobre amenazas cibernéticas.

Los CERTs, en cambio, son un grupo más específico de CSIRTs en tanto son aquellos que incorporan a "CERT" como marca registrada propiedad de la Universidad Carnegie Mellon. Los CSIRT que comparten el compromiso de la SEI (la Software

Engineering Institute) de mejorar la seguridad de las redes conectadas a Internet pueden solicitar autorización para usar la marca "CERT" en sus nombres.

Los CSIRTs pueden ser gubernamentales, comerciales, ONGs, y tienen una variedad de modelos organizacionales que los respaldan (centralizados, distribuidos, etc.).

Cuando se presenta un incidente de seguridad, un CSIRT debe cumplir con diferentes propósitos: **controlar y minimizar** cualquier tipo de daño a la organización y su información, junto con la preservación de **evidencia** sobre lo ocurrido y la documentación correspondiente. De esta forma, se conocerá el contexto del incidente, que permitirá determinar su origen y posibles consecuencias.

También debe coordinar las actividades para una **recuperación rápida** y eficiente de las actividades que se han visto afectadas, en conjunto con los equipos de TI, de manera que la organización pueda operar con normalidad en el menor tiempo posible y con el **menor impacto** tolerable.

Además, debe prevenir que eventos similares puedan ocurrir en el **futuro**, de tal forma que puedan erradicarse las causas raíz del incidente, junto con mantener una base de conocimientos que permita registrar las **lecciones aprendidas** de estos sucesos, con el objetivo de que no se repitan y si esto sucede, se pueda contar con un antecedente de la solución o soluciones posibles.

Una función más incluye actividades para **compartir información** relacionada con incidentes de seguridad con otros CSIRT, con fines de difusión, e intentando mitigar el impacto de nuevas amenazas, vulnerabilidades o ataques.

En el cuadro se pueden observar algunas iniciativas en materia de seguridad a nivel nacional, regional y global.

Iniciativas nacionales, regionales y globales

INICIATIVA	ALCANCE
LACNIC CSIRT– Warning, Advice and Reporting Point *Regional*	Centro de respuesta a incidentes de seguridad para la comunidad de LACNIC. https://csirt.lacnic.net
Foro de Seguridad en redes (LACSEC) de LACNIC	Espacio a nivel regional desde 2006. El grupo hoy integra el espacio del Foro Técnico de LACNIC. LACSEC **es el foro de seguridad en redes que siempre se enfocó en temas de seguridad desde un punto de vista técnico.**
LAC CSIRT de LACNIC	Grupo de trabajo para intercambio de experiencias vinculadas a los temas de seguridad entre actores de América Latina y el Caribe. A través del conocimiento e intercambio entre los participantes **se busca fortalecer a la región en la prevención y mitigación del impacto de incidentes de seguridad informática.**
Proyecto AMPARO de LACNIC *Regional*	Propicia **la adopción de prácticas de seguridad informática y brinda conceptos técnicos** para la creación de los Centros de Respuesta a Incidentes de Seguridad Informática (CSIRT).
CERT Nacional de Brasil *Nacional*	CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. https://www.cert.br/
FIRST *Global*	Es una organización internacional que **nuclea a más de 500 CERTs/CSIRTs** a nivel mundial que manejan cooperativamente incidentes de seguridad informática y promueven programas de prevención de incidentes. https://www.first.org/

En los últimos años se han elaborado modelos relevantes de análisis de las capacidades en materia de ciberseguridad en el sector público. Mencionaremos solamente tres, que consideramos los más robustos:

- el desarrollado por el Banco Interamericano de Desarrollo (el BID), en conjunto con la OEA y el Centro de Construcción de Ciber-Capacidades de Oxford;
- el propuesto por la Unión Internacional de las Telecomunicaciones (ITU);
- y el planteado por el Instituto Potomac, con apoyo de la OEA, denominado “Índice de Preparación Cibernética 2.0”.

En general, estos estudios han dejado en evidencia que la tendencia general en la región es el paulatino desarrollo de capacidades en ciberseguridad, pero que queda mucho trabajo por hacer. Por ejemplo, han permitido identificar que cuatro de cada cinco países de la región no cuentan con estrategias de ciberseguridad o planes de protección de infraestructura crítica, mientras que dos de cada tres no cuentan con un centro de comando y control de seguridad cibernética, según el BID en 2016.

El modelo de madurez en el que se basa el BID fue desarrollado por el **Software Engineering Institute**. En el año 2015 la Universidad de Oxford indaga en cinco dimensiones: política, cultura, educación, legislación y tecnología, dentro de ellas existen indicadores para medir el grado de madurez, en 2016 la aplicación de esta metodología fue reflejada en un informe del BID para demostrar los distintos niveles de desarrollo de ciberseguridad en la región.

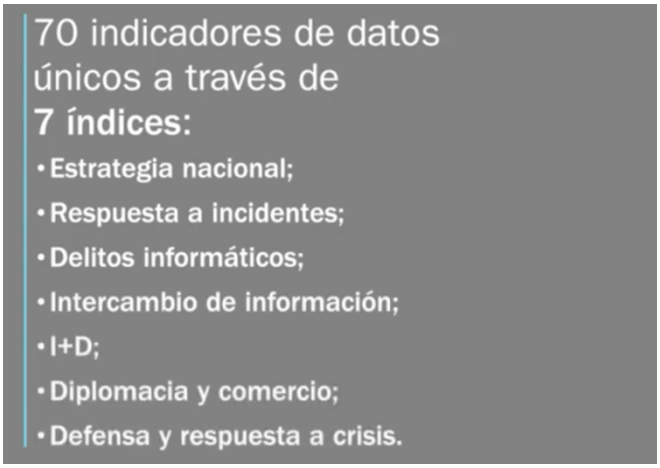
El modelo de la ITU, en tanto, se denomina Índice Mundial de Ciberseguridad. Lo que se evalúa es el "compromiso" de los países en materia de ciberseguridad de acuerdo con los cinco pilares de la Agenda sobre Ciberseguridad Global: medidas jurídicas, medidas técnicas, medidas organizativas, medidas de capacitación y medidas de cooperación. Como en el primer caso, se basa en una especie de encuesta online, sobre la base de un autodiagnóstico, que la ITU le solicita a cada país socio a partir de un cuestionario.

Se mencionará ahora el estudio del instituto Potomac. El índice de preparación cibernética 2.0. en el que se basa este estudio tiene dos componentes principales:

- en primer lugar, está diseñado para informar a los líderes nacionales de las medidas que deben tener en cuenta para a proteger a sus países cada vez más conectados y el potencial de crecimiento del PIB, mediante la evaluación objetiva de la madurez y el compromiso de cada país con la seguridad cibernética y la resiliencia.

- En segundo lugar, el índice de preparación cibernética 2.0. define lo que significa para un país estar “preparado cibernéticamente” y establece los componentes básicos de la preparación cibernética en un plan accionable que sea seguido por los países. La metodología del índice de preparación cibernética 2.0. representa una herramienta útil, única y fácil de usar para evaluar la brecha entre la postura de seguridad cibernética actual de una nación y las capacidades cibernéticas nacionales necesarias para lograr su visión económica.

El modelo desarrollado y empleado para este análisis incluye más de setenta indicadores de datos únicos a través de los índices que se muestran en la imagen.



Esta aproximación no es novedosa, y recoge la discusión generada en el seno de la **Freedom Online Coalition**, coalición internacional de países que declara como su objeto principal la promoción de la libertad en Internet.

Dentro de esta coalición, se formó un grupo de trabajo denominado “Una Internet abierta y segura”, que se abocó a construir una nueva definición de ciberseguridad con el objetivo de subirle el perfil a los derechos humanos para su consideración integral en la formulación de políticas públicas. Así, el grupo arribó al preámbulo y definición que se observa. Al fin y al cabo, se considera que el futuro del concepto de ciberseguridad desde un enfoque de derechos humanos no sólo apunta a proteger ciertos atributos de la información funcionales a estos, sino también a asegurar que el ciberespacio sea un ambiente fértil para el desarrollo de las personas, permitiendo a la humanidad alcanzar nuevos estándares de libertad y dignidad.

Es posible afirmar, que no existen derechos humanos determinados/ particulares/ específicos/ puntuales que se protejan en el ciberespacio, sino más bien que todos ellos tienen reconocimiento y protección en este ambiente, sin excepción. Sin embargo, existen algunos derechos que tienen particular relevancia en el ciberespacio, por estar vinculados estrechamente a la información, en sus diversas miradas y manifestaciones. Estos derechos son los de privacidad, libertad de expresión e información, complementados con los de seguridad y libertad personal y no discriminación.

La interacción de los derechos humanos y los diversos conceptos y tópicos sobre ciberseguridad es compleja y no siempre clara, puesto que los conceptos de ciberseguridad y derechos humanos se relacionan en diversos niveles. Se destaca principalmente, que ambos se complementan en una relación virtuosa en la medida que la ciberseguridad sea funcional a la protección de la privacidad, acceso a la información o libertad de expresión y seguridad personal entre otros derechos.