

MINUTA

Materia	El Estado de madurez en ciberseguridad de Chile, a partir del informe "Ciberseguridad. ¿Estamos preparados en América Latina y el Caribe?" (OEA y BID; 2016).
Fecha	Octubre, 2018
Autor	Jessica Matus

INTRODUCCIÓN:

A partir de un modelo desarrollado en los años 2014 y 2015 por el Centro Global de Capacidad en Ciberseguridad, de la Universidad de Oxford (Reino Unido), la OEA junto con el Banco Interamericano de Desarrollo (BID) desarrollaron, el año 2016, un informe en que se aplica el *modelo de madurez* desarrollado por el Centro, en el que se evalúa una serie de dimensiones (formadas por factores, y éstas –a su vez– por aspectos) utilizando *criterios de madurez*, que reflejan el estado de avance en que se encuentran estas dimensiones, con el fin de otorgar una visión global y comprensiva del estado de ciberseguridad en el país sometido a análisis.

EVALUACIÓN A CHILE:

- El informe, al referirse a nuestro país, comienza señalando que Chile "no ha emitido una estrategia nacional de seguridad cibernética", sin embargo, "la sensibilización entre las instituciones gubernamentales es generalizada. La infraestructura gubernamental presenta tecnología de seguridad actualizada y las partes interesadas pertinentes regularmente analizan los activos y vulnerabilidades de la Infraestructura Crítica Nacional. El Estado también coordina la planeación de gestión de crisis y ha puesto en marcha medidas de redundancia".
- Destacan también las labores compartidas en ciberseguridad que tienen las FF.AA; pero advierte la falta de "una estructura central de mando y control". Consideran como desafío para Chile "el fortalecimiento de su capacidad de respuesta a incidentes".
- Respecto al marco legal, se menciona el DS N° 1.299 y las leyes N°s 19.223 y 19.628. Indica que los privados no están obligados a divulgar las violaciones sobre ciberseguridad, pero que el gobierno trabaja con ellos para informar y responder a incidentes cibernéticos. Según informaron las autoridades, en Chile los ataques cibernéticos más comunes son el *phishing*, el *malware* y la piratería informática. La investigación de estos delitos queda a cargo del Departamento de Investigación de Organizaciones Criminales (OS-9) y el Laboratorio de Criminalística (LABORCAR) de Carabineros.
- Finalmente, se deja en claro que "la mentalidad de seguridad cibernética es inconsistente en la sociedad chilena", es decir, **la sociedad chilena no ha adoptado una cultura de seguridad cibernética**. En todo caso, rescatan las campañas gubernamentales (*Internet Segura* del MINEDUC [2013]; y *Consumidor Digital*) y los títulos entregados por la Universidad de Chile en esta materia. En todo caso, "el sector privado se ha vuelto cada vez más consciente de los riesgos de seguridad cibernética y ha puesto en marcha planes para abordarlos".

ESTADOS DE MADUREZ Y CUMPLIMIENTO DE CADA UNO DE ELLOS EN CHILE.

Luego, se analiza el estado de madurez de cada dimensión. Se reconocen cinco niveles de madurez en ciberseguridad:

Estado de madurez	Descripción
Inicial	En este nivel, o nada existe, o es de naturaleza muy embrionaria. También incluye un pensamiento o una observación acerca de un problema, pero no una acción.
Formativo	Algunas características del subfactor han comenzado a crecer y ser formuladas, pero pueden ser casuales, desorganizadas, mal definidas o simplemente “nuevas”
Establecido	Los elementos del subfactor están establecidos y funcionando. Sin embargo, no se ha considerado bien la asignación relativa de recursos. Ha habido poca toma de decisiones de compensación en relación con la inversión relativa en los distintos elementos del subfactor. Pero el subfactor es funcional y está definido.
Estratégico	Estratégico no significa importante; más bien, se trata de una selección. Al nivel nacional se han elegido las partes del subfactor que son clave, así como aquellas que son menos importantes para la organización/país en particular. Estas elecciones toman en consideración un resultado esperado, una vez implementado, que contiene circunstancias particulares y otros objetivos nacionales existentes.
Dinámico	A nivel dinámico, existen mecanismos claros para alterar la estrategia en función de las circunstancias imperantes. Por ejemplo, la tecnología del entorno de amenazas, conflicto global, un cambio significativo en un área de interés (por ejemplo, la delincuencia cibernética o privacidad). Organizaciones dinámicas han desarrollado métodos para cambiar las estrategias, de acuerdo con una manera de “sentir y responder”. La toma de decisiones rápida, la reasignación de los recursos y la atención constante a los cambios del entorno son las características de este nivel.

El estado de madurez, según dimensión, factor, y aspecto; son las siguientes:

Dimensión	Factor	Aspectos
Política y estrategia	Estrategia nacional de seguridad cibernética oficial o documentada	<ul style="list-style-type: none"> – Desarrollo de la estrategia: <u>Formativo</u>. – Organización: <u>Formativo</u>. – Contenido: <u>Formativo</u>.
	Defensa cibernética	<ul style="list-style-type: none"> – Estrategia: <u>Formativo</u>. – Organización: <u>Formativo</u>. – Coordinación: <u>Formativo</u>.
Cultura y sociedad	Mentalidad de seguridad cibernética	<ul style="list-style-type: none"> – En el gobierno: <u>Formativo</u>. – En el sector privado: <u>Establecido</u>. – En la sociedad: <u>Formativo</u>.
	Conciencia de seguridad cibernética	<ul style="list-style-type: none"> – Sensibilización: <u>Formativo</u>.

	Confianza en el uso de Internet	<ul style="list-style-type: none"> – En los servicios en línea: <u>Formativo</u>. – En el gobierno electrónico: <u>Formativo</u>. – En el comercio electrónico: <u>Establecido</u>.
	Privacidad en línea	<ul style="list-style-type: none"> – Normas de privacidad: <u>Estratégico</u>. – Privacidad del empleado: <u>Formativo</u>.
Educación	Disponibilidad nacional de la educación y formación cibernéticas	<ul style="list-style-type: none"> – Educación: <u>Formativo</u>. – Formación: <u>Formativo</u>.
	Desarrollo nacional de la educación de seguridad cibernética	– Desarrollo nacional de la seguridad cibernética: <u>Inicial</u> .
	Formación de iniciativas educativas públicas y privadas	– Capacitación de empleados en seguridad cibernética: <u>Formativo</u> .
	Gobernanza corporativa, conocimiento y normas	– Comprensión de la seguridad cibernética por parte de empresas privadas y estatales: <u>Establecido</u> .
Marcos legales	Marcos jurídicos de seguridad cibernética	<ul style="list-style-type: none"> – Para la seguridad de las TIC: <u>Establecido</u>. – Privacidad, protección de datos y otros derechos humanos: <u>Establecido</u>. – Derecho sustantivo de delincuencia cibernética: <u>Establecido</u>. – Derecho procesal de delincuencia cibernética: <u>Estratégico</u>.
	Investigación jurídica	<ul style="list-style-type: none"> – Cumplimiento de la ley: <u>Establecido</u>. – La fiscalía: <u>Establecido</u>. – Tribunales: <u>Formativo</u>.
	Divulgación responsable de la información	– Divulgación responsable de la información: <u>Inicial</u> .
Tecnologías	Adhesión a las normas	<ul style="list-style-type: none"> – Aplicación de las normas y prácticas mínimas aceptables: <u>Formativo</u>. – Adquisiciones: <u>Formativo</u>. – Desarrollo de software: <u>Formativo</u>.
	Organizaciones de coordinación de seguridad cibernética	<ul style="list-style-type: none"> – Centro de mando y control: <u>Formativo</u>. – Capacidad de respuesta a incidentes: <u>Formativo</u>.
	Respuesta a incidentes	<ul style="list-style-type: none"> – Identificación y designación: <u>Formativo</u>. – Organización: <u>Formativo</u>. – Coordinación: <u>Formativo</u>.
	Resiliencia de la infraestructura nacional	<ul style="list-style-type: none"> – Infraestructura tecnológica: <u>Establecido</u>. – Resiliencia nacional: <u>Establecido</u>.
	Protección de la infraestructura crítica nacional	<ul style="list-style-type: none"> – Identificación: <u>Establecido</u>. – Organización: <u>Estratégico</u>. – Planeación de respuesta: <u>Formativo</u>. – Coordinación: <u>Formativo</u>. – Gestión de riesgos: <u>Formativo</u>.
	Gestión de crisis	<ul style="list-style-type: none"> – Planeación: <u>Formativo</u>. – Evaluación: <u>Formativo</u>.
	Redundancia digital	<ul style="list-style-type: none"> – Planeación: <u>Formativo</u>. – Organización: <u>Formativo</u>.
	Mercado de la ciberseguridad	– Tecnologías de seguridad cibernética: <u>Formativo</u> .

- Seguros de delincuencia cibernética: Establecido.

CAMBIOS METODOLÓGICOS.

Entre el CMM publicado el 2016 y este informe, se efectuaron cambios metodológicos por el Centro Global de Capacidad sobre Seguridad Cibernética en su Modelo de Madurez de Capacidad de Seguridad Cibernética (CMM), que principalmente se ven reflejados en la modificación de dimensiones y factores.

Por ejemplo, podemos señalar que en el CMM, los factores de *manejo de crisis, respuesta a incidentes y redundancia en las comunicaciones* son consideradas en la dimensión “Política y estrategia en ciberseguridad”; mientras que en el informe elaborado por la OEA y el BID, estos mismos factores son considerados en la dimensión “Tecnologías”.

Otra modificación importante es que el CMM considera que los esfuerzos en el desarrollo y ejecución de una estrategia nacional en ciberseguridad son una materia que requiere de la cooperación entre entes públicos y privados; mientras que el informe considera que la ejecución es intra-estatal y, en ese sentido, la cooperación que debe existir es esencialmente entre organismos estatales.

El detalle de las diferencias entre los factores del CMM y los considerados en el informe se encuentra en la tabla desarrollada más abajo.

CMM	Informe OEA&BID
<p>Dimensión N° 1: Política y estrategia en ciberseguridad.</p> <ul style="list-style-type: none"> – Estrategia nacional de ciberseguridad. – Respuesta a incidentes. – Protección a infraestructura crítica. – Manejo de crisis. – Defensa contra crisis. – Redundancia en las comunicaciones. 	<p>Dimensión N° 1: Política y estrategia.</p> <ul style="list-style-type: none"> – Estrategia nacional de seguridad cibernética. – Defensa cibernética.
<p>Dimensión N° 2: Cibercultura y sociedad.</p> <ul style="list-style-type: none"> – Actitud de ciberseguridad. – Confianza en el internet. – Entendimiento de los usuarios de la protección de su información personal en línea. – Mecanismos de reporte. – Medios y redes sociales. 	<p>Dimensión N° 2: Cultura y sociedad.</p> <ul style="list-style-type: none"> – Mentalidad de seguridad cibernética. – Conciencia de seguridad cibernética. – Confianza en el uso de Internet. – Privacidad en línea.
<p>Dimensión N° 3: Educación, entretenimiento y habilidades en ciberseguridad.</p> <ul style="list-style-type: none"> – Sensibilización. – Marco para la educación. 	<p>Dimensión N° 3: Educación.</p> <ul style="list-style-type: none"> – Disponibilidad nacional de la educación y formación cibernéticas. – Desarrollo nacional de la educación de seguridad cibernética.

<ul style="list-style-type: none"> – Marco para el entrenamiento profesional. 	<ul style="list-style-type: none"> – Formación e iniciativas educativas públicas y privadas. – Gobernanza corporativa, conocimiento y normas.
<p>Dimensión N° 4: Marcos legales y regulatorios.</p> <ul style="list-style-type: none"> – Marco legal. – Sistema de justicia criminal. – Marcos de cooperación formal e informal para combatir el cibercrimen. 	<p>Dimensión N° 4: Marcos legales.</p> <ul style="list-style-type: none"> – Marcos jurídicos de seguridad cibernética. – Investigación jurídica. – Divulgación responsable de información.
<p>Dimensión N° 5: Estándares, organizaciones y tecnologías.</p> <ul style="list-style-type: none"> – Adhesión a los estándares. – Resiliencia de las estructuras de internet. – Calidad de software. – Controles técnicos de seguridad. – Control criptográfico. – Mercado de ciberseguridad. – Divulgación responsable. 	<p>Dimensión N° 5: Tecnologías.</p> <ul style="list-style-type: none"> – Adhesión a las normas. – Organizaciones de coordinación de seguridad cibernética. – Respuesta a incidentes. – Resiliencia de la infraestructura nacional. – Protección de la Infraestructura Crítica Nacional (CNI). – Gestión de crisis. – Redundancia digital. – Mercado de la ciberseguridad.