

MINUTA

Materia	MODELO NACIONAL DE MADUREZ DE CAPACIDAD EN CIBERSEGURIDAD (CMM). Universidad de Oxford.
Fecha	Septiembre, 2018
Autor	Jessica Matus

1. RESUMEN EJECUTIVO.

El Global Cyber Security Capacity Center -Centro Global de Capacidad en Ciberseguridad (o Centro de Capacidad)- ha desarrollado un modelo orientado a las naciones para incrementar la escala y efectividad en la construcción de sus capacidades en ciberseguridad de manera sistemática y sustantiva.

Mediante este modelo, el Centro de Capacidad espera ayudar a promover un ciberespacio más innovador en apoyo del bienestar, el respeto a los derechos humanos y la prosperidad para todos.

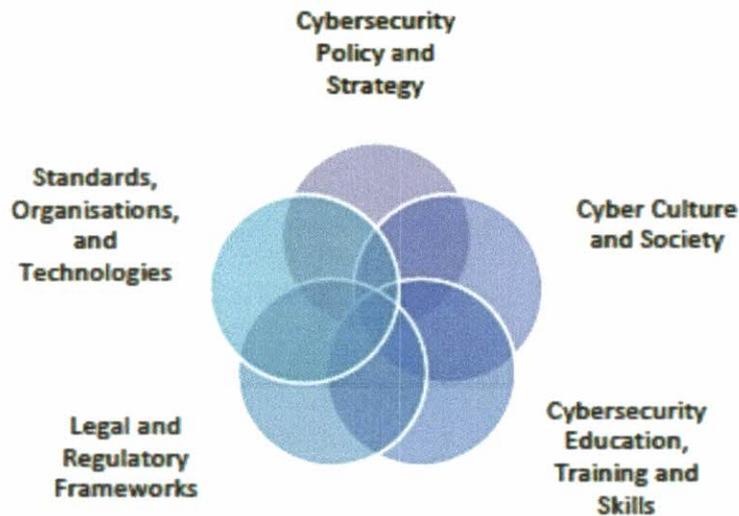
El modelo fue desarrollado en 2014 y entregado en 2015, incluyendo un diagnóstico regional para Latinoamérica y el Caribe (dirigido por la OEA y el BID). Estas revisiones se llevaron a cabo junto con varias organizaciones internacionales y ministerios líderes, y se convocó a stakeholders para obtener un entendimiento comprensivo sobre el nivel de madurez de la ciberseguridad nacional.

Durante estas revisiones, el Centro de Capacidad fue capaz de medir si el contenido del modelo era consistente con el panorama global de capacidades en ciberseguridad, así como determinar formas en las cuales se puede mejorar el contenido general, la estructura y el despliegue del modelo a través de las lecciones aprendidas. Se introdujeron cambios estructurales y no sustanciales; ciertos factores y aspectos fueron combinados o reconfigurados para mejorar la claridad y precisión del modelo.

2. INTRODUCCIÓN.

El Centro de Capacidad considera que la ciberseguridad comprende cinco dimensiones:

- 1) El diseño de una política y estrategia de ciberseguridad;
- 2) Promover en la sociedad una cultura de ciberseguridad responsable;
- 3) Desarrollar conocimiento en ciberseguridad;
- 4) Crear marcos legales y regulatorios que sean efectivos; y
- 5) Controlar riesgos mediante estándares, organizaciones y tecnologías.



Estas dimensiones cubren la amplia extensión a considerar cuando se trata de mejorar las capacidades en ciberseguridad; y a su vez, estas dimensiones pueden superponerse entre sí en ciertos temas. Dentro de cada una, existen varios factores, aspectos, etapas e indicadores de capacidad en ciberseguridad:

- **Dimensiones:** Cada dimensión representa un grupo de capacidad en ciberseguridad que el Centro de Capacidad analiza. Representa los distintos “lentes” de investigación a través de los cuales se estudian las capacidades en ciberseguridad.
- **Factores:** Dentro de cada dimensión existen distintos factores, los cuales describen en qué consiste tener capacidades en ciberseguridad. Son elementos que contribuyen para mejorar la madurez en las capacidades en ciberseguridad. La mayoría de factores se componen de una serie de aspectos que estructuran el contenido del factor, otros son más limitados y no tienen aspectos específicos.
- **Aspectos:** Cada factor se presenta como una serie de aspectos, que representan diferentes componentes del factor. Los aspectos representan un método de organización para dividir los indicadores en grupos más pequeños que son más fáciles de comprender. El número de aspectos depende de los temas que surgen en el contenido del factor y la complejidad global del factor. Cada aspecto se compone de una serie de indicadores dentro de las 5 etapas de madurez.
- **Etapas:** Definen en qué grado un país ha progresado en relación a un determinado factor o aspecto en su capacidad en ciberseguridad. Cada etapa se caracteriza de esta forma:
 - Puesta en marcha: No existe madurez en ciberseguridad, o aún es embrionaria. Pueden haber discusiones iniciales sobre la construcción de capacidades en ciberseguridad, pero no se han tomado acciones concretas.

- **Formativa:** Algunas características de los aspectos se han comenzado a aplicar y a formularse, pero podrían ser ad-hoc, desorganizadas, pobremente diseñadas, o simplemente nuevas. La evidencia de esta actividad puede ser claramente demostrada.
- **Establecida:** Los elementos de los aspectos están en su lugar y trabajando. Sin embargo, no hay una profunda consideración sobre la asignación relativa de recursos.
- **Estratégica:** Se han tomado decisiones sobre qué partes de cada aspecto son o no importantes para una organización o país en particular.
- **Dinámica:** Existen mecanismos claros para alterar las estrategias en ciberseguridad, dependiendo de las circunstancias existentes como la tecnología, medioambiente, conflictos globales o un cambio significativo en un área de interés.
- **Indicadores:** Representan la parte más elemental de la estructura del modelo. Cada indicador describe los pasos, acciones, o bloques de construcción que indican la madurez de una etapa específica en distintos aspectos, factores y dimensiones.

3. MODELO NACIONAL DE MADUREZ DE CAPACIDAD EN CIBERSEGURIDAD.

3.1. DIMENSIÓN N° 1: ESTRATEGIAS Y POLÍTICA DE CIBERSEGURIDAD.

Esta dimensión explora la capacidad del país para desarrollar y entregar estrategias de ciberseguridad y mejorar la resiliencia de su ciberseguridad mediante una mejor respuesta de incidentes, gestión de crisis, redundancia, y capacidad de protección de su infraestructura crítica. La entrega de ciberseguridad debe incluir capacidad de alerta temprana, disuasión, resistencia y recuperación. Será efectiva una política de ciberseguridad en la prestación de capacidades de defensa y resiliencia nacional, manteniendo los beneficios de un ciberespacio vital para el gobierno, los negocios internacionales y la sociedad en general.

a) Estrategia nacional de ciberseguridad.

Esencial, en tanto ayuda a priorizar la ciberseguridad como un área política importante, determina responsabilidades, encarga la ciberseguridad clave a actores gubernamentales y no gubernamentales, y dirige la colocación de recursos a prioridades y cuestiones de ciberseguridad que estén emergiendo o ya existentes.

Este factor considera tres aspectos: el desarrollo de una estrategia nacional de ciberseguridad¹; la existencia de un programa de coordinación en ciberseguridad (órgano con presupuesto consolidado); y el contenido de la estrategia nacional de ciberseguridad, vinculado estrechamente a los riesgos, prioridades y objetivos

¹ Además de la asignación de autoridades de aplicación en todos los sectores y la sociedad civil y una comprensión de los riesgos y las amenazas de ciberseguridad nacional que impulsa el desarrollo de capacidades a nivel nacional.

nacionales, como la sensibilización pública, mitigación del cibercrimen, capacidad de respuesta a incidentes y protección de la infraestructura nacional crítica.

b) Respuesta a incidentes.

Se relaciona a la capacidad gubernamental para identificar y determinar características de los incidentes a nivel nacional de forma sistemática. También revisa la capacidad del gobierno para organizar, coordinar y operar respuestas a incidentes.

Este factor considera cuatro aspectos: si existe un registro central a nivel nacional de identificación de incidentes; si existe un órgano central mandatado a recoger información sobre incidentes (y su relación con el sector público y privado para respuesta de nivel nacional); la existencia de una respuesta coordinada a nivel nacional (con responsabilidades y roles claramente determinados); y la capacidad operativa y técnica de la organización para las respuestas a incidentes (servicios, procesos, recursos, herramientas)

c) Protección de infraestructura crítica.

Se relaciona con la capacidad gubernamental para identificar infraestructura crítica (IC) y los riesgos asociadas a ésta, participar en la planificación de respuestas y la protección de los activos críticos, facilitar la interacción de calidad con los dueños de IC, y permitir una gestión de riesgos comprensivo a nivel general que incluya el planeamiento de respuestas.

Considera tres aspectos: la existencia de una lista general de activos de IC, sus riesgos y la práctica de auditorías; la existencia de un mecanismo de colaboración formal entre ministerios de gobierno y los dueños de dichos activos; y si la ciberseguridad está integrada con las prácticas generales de manejo de riesgos, medidas de seguridad para continuidad del negocio, procedimientos y procesos de protección de información para la planificación de respuesta ante un ataque con el apoyo de soluciones técnicas adecuadas de seguridad.

d) Gestión de crisis.

Considera la planificación para el manejo de crisis, conduciéndola a necesidades especializadas, ejercicios de entrenamiento y simulaciones que producen resultados escalables para el desarrollo de decisiones estratégicas. Mediante técnicas cualitativas y cuantitativas, los procesos de evaluación de ciberseguridad buscan producir resultados estructurados y medibles que permitan proponer recomendaciones a los responsables de la formulación de políticas y a otras partes interesadas, e informen sobre la implementación de la estrategia nacional, así como para guiar las asignaciones presupuestarias.

e) Consideración de ciberdefensa.

Se relaciona con la capacidad del gobierno para diseñar e implementar una estrategia de ciberdefensa, y lidere su implementación a través de un organismo designado para tareas de ciberdefensa. También revisa el nivel de coordinación

entre varios actores de los sectores público y privado para responder a ataques en sistemas de información estratégicos e infraestructura crítica nacional.

Considera tres aspectos: la existencia de una estrategia nacional de ciberdefensa; la designación de un organismo de gobierno responsable de la defensa en caso de conflictos cibernéticos; y la coordinación en respuesta a ataques maliciosos en sistemas de información estratégicos e infraestructura crítica nacional.

- f) Redundancia en la comunicación: Este factor se relaciona con la capacidad del gobierno para identificar y mapear la redundancia digital y de comunicaciones entre partes interesadas. La redundancia digital prevé un sistema de ciberseguridad en que la duplicación y fallo de cualquier componente esté salvaguardado por el respectivo respaldo. La mayoría de estos respaldos estarán aislados, pero listos para ser usados en redes digitales; y otros serán no digitales.

3.2. DIMENSIÓN N°2: CIBERCULTURA Y SOCIEDAD.

Esta dimensión revisa elementos importantes e una cultura responsable de ciberseguridad, como la comprensión de los riesgos, el nivel de confianza en los servicios de Internet, servicios de gobierno electrónico y el comercio electrónico, comprensión de la protección de datos en línea. Mecanismos de información como canales para informar a los usuarios sobre ciberdelincuencia. Examina también el rol de los medios de comunicación y las redes sociales en la formación de los valores de ciberseguridad, actitudes y comportamiento.

- a) Actitud o Mentalidad de ciberseguridad (mind-set).

Este factor evalúa el grado en que se da prioridad a la ciberseguridad y si es integrada en los valores, actitudes y prácticas habituales del gobierno, el sector privado, y los usuarios a través de la sociedad en general. Una mentalidad o estructura mental de ciberseguridad consiste en valores, actitudes y prácticas, incluyendo hábitos, de usuarios individuales, expertos, y otros actores en el ecosistema de la ciberseguridad, que incrementan la resiliencia de los usuarios a amenazas a su propia seguridad.

Considera tres aspectos: si todas las agencias de gobierno (independiente de su nivel) han adoptado proactivamente una actitud de ciberseguridad; si todas las agencias del mundo privado han adoptado proactivamente una actitud de ciberseguridad en la industria y el comercio; y si la sociedad ha adoptado una actitud de ciberseguridad.

- b) Confianza en Internet.

Este factor evalúa el nivel de confianza del usuario en el uso de servicios en línea, en general; y el uso de plataformas en línea de gobierno y comercio, en particular.

Considera tres aspectos: si el usuario confía en los servicios en línea, independiente si existe un programa coordinado o un operador de Internet que promueva esa confianza; si existen servicios de gobierno en línea, y si se confía en la seguridad de

dichos servicios; y si existen servicios de comercio en línea, y si se entregan en un ambiente seguro y confiado por los usuarios.

- c) Entendimiento de los usuarios de la protección de su información personal en línea: Este aspecto evalúa si los usuarios de Internet y las partes interesadas en los sectores público y privado reconocen y entienden la importancia de la protección de la información personal en línea, y si están sensibilizados con su derecho a la privacidad.
- d) Mecanismos de reporte: Este aspecto explora la existencia de mecanismos de reporte funcionales, como canales para los usuarios para reportar delitos como fraude online, ciber-bullying, abuso contra menores en línea, suplantación de identidad, filtraciones de privacidad y seguridad, entre otros.
- e) Medios de comunicación y redes sociales: Este aspecto explora si la ciberseguridad es una materia tratada de forma común en los medios, y un tema de discusión en redes sociales. Más específicamente, este aspecto trata sobre el rol de los medios al entregar información sobre ciberseguridad al público, y de esa forma, modela los valores y actitudes sobre la ciberseguridad, y su comportamiento en línea².

3.3. DIMENSIÓN N° 3: EDUCACIÓN, ENTRENAMIENTO Y HABILIDADES EN CIBERSEGURIDAD.

a) Sensibilización.

Este factor se enfoca en la prevalencia y diseño de programas para sensibilizar sobre riesgos y amenazas en ciberseguridad, y cómo abordarlos.

Considera dos aspectos: la existencia de un programa nacional coordinado de sensibilización en materias de ciberseguridad, que abarque un amplio espectro demográfico y de tópicos, desarrollado a partir de consultas con partes interesadas de distintos sectores; y los esfuerzos de las autoridades para sensibilizar en materias de ciberseguridad en las esferas pública, privada, académica y de la sociedad civil. Así como los riesgos de ciberseguridad a los que se dirigen.

b) Marco para la educación.

Este factor identifica la importancia de una educación de calidad en materia de ciberseguridad, que ésta sea ofrecida efectivamente y la existencia de educadores calificados. Más específicamente, examina la necesidad de mejorar la educación en ciberseguridad a nivel nacional e institucional, y la colaboración entre gobierno e industria para asegurar que las inversiones en educación satisfagan las necesidades del entorno de ciberseguridad en todos los sectores.

Considera dos aspectos: la existencia de una ofertas educativas en ciberseguridad y los programas de cualificación de los educadores disponibles, basados en un entendimiento de los riesgos actuales y las habilidades requeridas; y la

² Los acontecimientos de los últimos meses en relación a la filtración de información ha evidenciado una brecha importante en la forma de abordar las materias tecnológicas por parte de los medios de comunicación.

coordinación y recursos para el desarrollo y mejora de los marcos educativos en ciberseguridad, con un presupuesto asignado y un gasto basado en la demanda nacional.

c) Marco para la formación profesional.

Este factor identifica la disponibilidad y provisión de programas de formación en ciberseguridad, construyendo un equipo de profesionales en ciberseguridad. Más específicamente, revisa la adopción del entrenamiento en ciberseguridad en niveles horizontales y verticales, además de la transferencia de conocimiento entre organizaciones y cómo ello se traduce en un desarrollo continuo de habilidades.

Considera dos aspectos: el desarrollo, disponibilidad y provisión de programas de formación en ciberseguridad que mejoren habilidades y capacidades; y la existencia de empleados con entrenamiento certificado en cuestiones, procesos, planeamiento y análisis de ciberseguridad a través de programas de formación y transferencia de conocimiento dentro de las organizaciones.

3.4. **DIMENSIÓN N° 4: MARCOS LEGALES Y REGULATORIOS.**

a) Marco legal.

Este factor se refiere a los distintos marcos normativos y regulación que existen en materia de ciberseguridad, incluyendo: marcos legales de seguridad en TICs; privacidad, libertad de expresión y otros derechos humanos en línea; protección de datos personales; protección de menores, protección a consumidores; propiedad intelectual; y legislación sobre cibercrimes a nivel sustantivo y procesal.

Considera los siguientes ocho elementos:

- 1) La existencia e implementación de legislación comprensiva de seguridad en TICs y marcos regulatorios.
- 2) La extensión en que la legislación interna garantiza que los derechos humanos se protegen en línea, incluyendo los derechos a la privacidad, libertad de expresión, libertad de información, y libertad de reunión y asociación.
- 3) La existencia y aplicación de una legislación de protección de datos personales.
- 4) La existencia de legislación que proteja a los menores de edad en línea, incluyendo la protección de sus derechos en línea y la criminalización del abuso de menores en línea.
- 5) La existencia y aplicación de una legislación que proteja a los consumidores en línea del fraude y otras formas de malas prácticas en el comercio.
- 6) La existencia y aplicación de legislación que proteja la propiedad intelectual en línea.
- 7) La existencia de legislación que tipifique una serie de cibercrimes en una legislación específica o en la legislación criminal en general.

- La aplicación del derecho procesal penal general para la investigación del cibercrimen, la legislación aplicable en materia probatoria por cibercrímenes, y los delitos que involucren pruebas electrónicas.

b) Sistema de justicia criminal.

Este factor estudia la capacidad de las policías para investigar el cibercrimen, y de los fiscales para presentar cargos por delitos informáticos y evidencia o prueba electrónica. Finalmente, se refiere a la capacidad de los tribunales para dirigir casos de delitos cibernéticos y aquellos en que se presente evidencias electrónicas.

Considera tres aspectos: si las **policías** tienen formación para la investigación y el manejo de delitos informáticos y en aquellos casos con evidencias electrónicas, y si tienen los suficientes recursos humanos, procesales y tecnológicos; si los **fiscales** han recibido entrenamiento en el manejo de casos de cibercrimen y en aquellos casos que involucren evidencia electrónica, y si cuentan con los suficientes recursos humanos, procesales y tecnológicos; y si los **tribunales de justicia** tienen los suficientes recursos y entrenamiento para asegurar una efectiva y eficiente persecución de los delitos informáticos y para manejar los casos en que se presente evidencia electrónica.

c) Marcos de cooperación formal e informal para combatir la ciberdelincuencia.

Este factor se refiere a la existencia y funcionalidad de mecanismos formales e informales que permitan la cooperación entre actores internos y externos para impedir y combatir el cibercrimen.

Considera dos aspectos: La existencia y efectividad de mecanismos de cooperación formales para combatir el cibercrimen, entre actores estatales e internacionales, incluyendo asistencia legal mutua y procedimientos de extradición; y la existencia y efectividad de mecanismos informales de cooperación para combatir el cibercrimen, tanto a nivel nacional como internacional, y tanto dentro como entre los sectores público y privado.

3.5. DIMENSIÓN N° 5: ESTÁNDARES, ORGANIZACIONES Y TECNOLOGÍAS.

a) Adhesión a los estándares. Este factor analiza la capacidad del gobierno para diseñar, adaptar e implementar estándares de ciberseguridad y buenas prácticas, especialmente aquellas relacionadas con la adopción de procedimientos y el desarrollo de software.

Considera tres aspectos: La adopción de estándares y buenas prácticas en ciberseguridad de forma general en el sector público y en las organizaciones con IC; la implementación de estándares en prácticas de adquisiciones o compras; y la implementación de estándares en el desarrollo de software.

b) Resiliencia de las estructuras de Internet. Este factor se refiere a la existencia de servicios de Internet confiables y a la infraestructura de Internet nacional, así como a la rigurosidad de los procesos de seguridad en los sectores público y privado.

También examina el control que el gobierno tenga sobre la infraestructura del Internet, y la medida en que las redes y sistemas son subcontratados.

- c) Calidad de software: Este factor examina la calidad de desarrollo de software y los requerimientos funcionales en los sectores público y privado. Además, analiza la existencia y mejora de políticas en los procesos de actualización de software y mantenimiento, basados en evaluación de riesgos y la criticidad de los servicios.
- d) Controles técnicos de seguridad: Este factor revisa la evidencia recolectada sobre el despliegue de controles técnicos de seguridad por parte de los usuarios, el sector público y privado; y si el conjunto de control de ciberseguridad técnico se basa en marcos de ciberseguridad establecidos.
- e) Control criptográfico: Este factor verifica el desarrollo de técnicas criptográficas en todos los sectores y usuarios para la protección de sus datos guardados o en transferencia, y en qué medida dichos controles calzan con estándares y directrices internacionales, y si están actualizadas.
- f) Mercado de ciberseguridad. Este factor analiza la disponibilidad y desarrollo de tecnologías en ciberseguridad que sean competitivas, y productos de seguros.
Considera dos aspectos: La existencia de un mercado nacional de tecnologías en ciberseguridad que se ajusta a las necesidades nacionales; y la existencia de un mercado de seguros cibernéticos, su cobertura y los productos disponibles de parte de varias organizaciones.
- g) Divulgación responsable: Este factor explora el establecimiento de un marco de divulgación responsable para la recepción y diseminación de información sobre vulnerabilidades a través de distintos sectores, y si existe la suficiente capacidad para revisar y actualizar continuamente ese marco.

El documento incluye una matriz de análisis de la situación de cada país en las dimensiones, factores y aspectos indicados, con el objeto de determinar en qué estado se encuentra:

- Puesta en marcha
- Formativa
- Establecida
- Estratégica
- Dinámica