El Modelo de Madurez de la Capacidad de Ciberseguridad

El Centro Global de Capacidad en Seguridad Cibernética *(GCSCC, por sus siglas en inglés)*[33] de la Universidad de Oxford, en consulta con más de 200 expertos internacionales provenientes de gobiernos, la sociedad civil y la academia, desarrolló el Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones *(CMM, por sus siglas en inglés)*. Se trata de un modelo que busca ofrecer una evaluación del nivel de madurez de las capacidades de ciberseguridad de un país, asignándole una etapa específica que corresponde a su grado de logro en materia de ciberseguridad. Las cinco etapas de madurez, que se fijan por medio de una evaluación, van desde la más básica *(inicial)* hasta la más avanzada *(dinámica)*.

Las cinco etapas se definen[34] como sigue (véase el gráfico 1):

- ***Inicial:*** En esta etapa no existe madurez en ciberseguridad o bien se encuentra en un estadio muy embrionario. Puede haber discusiones iniciales sobre el desarrollo de capacidades de ciberseguridad, pero no se han tomado medidas concretas. Falta evidencia observable de la capacidad de seguridad cibernética.

- ***Formativa:*** Algunos aspectos han comenzado a crecer y formularse, pero pueden ser ad hoc, desorganizados, mal definidos, o simplemente nuevos. Sin embargo, se puede demostrar claramente evidencia de este aspecto.

- ***Consolidada:*** Los indicadores están instalados y funcionando. Sin embargo, no se le ha dado mucha consideración a la asignación de recursos. Se han tomado pocas decisiones acerca de los beneficios con respecto a la inversión relativa en este aspecto. Pero la etapa es funcional y está definida.

- ***Estratégica:*** En esta etapa se han tomado decisiones sobre qué indicadores de este aspecto son importantes y cuáles lo son menos para la organización o el Estado en particular. La etapa estratégica refleja el hecho de que estas elecciones se han realizado condicionadas por las circunstancias particulares del Estado o de las organizaciones.

- ***Dinámica:*** En esta etapa existen mecanismos claros para alterar la estrategia en función de las circunstancias prevalentes, como la sofisticación tecnológica del entorno de amenaza, el conflicto global o un cambio significativo en un área de preocupación (por ejemplo, delito informático o privacidad). Las organizaciones dinámicas han desarrollado métodos para cambiar las estrategias con calma. Sin embargo, la rápida toma de decisiones, la reasignación de recursos y la atención constante al entorno cambiante son características de esta etapa.

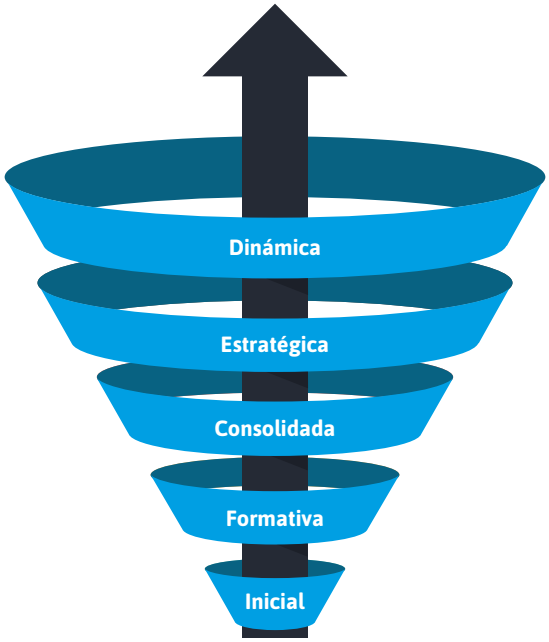

Gráfico 1: Las cinco etapas de madurez de la capacidad de ciberseguridad

La evaluación de los niveles de madurez se divide en cinco dimensiones (véase el gráfico 2) que corresponden a aspectos esenciales y específicos de la ciberseguridad, entre ellos: (i) política y estrategia de ciberseguridad; (ii) cultura cibernética y sociedad; (iii) educación, capacitación y habilidades en ciberseguridad; (iv) marcos legales y regulatorios; y (v) estándares, organizaciones y tecnologías. Estos se subdividen en un conjunto de factores que describen y definen lo que significa poseer capacidad de seguridad cibernética en cada factor, e indican cómo mejorar la madurez.

La siguiente tabla detalla cada uno de los factores que comprenden las dimensiones:

Dimensión 1 Política y Estrategia de Ciberseguridad (Diseño de estrategia y resiliencia de ciberseguridad)	**D1.1** Estrategia Nacional de Ciberseguridad **D1.2** Respuesta a Incidentes **D1.3** Protección de Infraestructura Crítica (IC) **D1.4** Gestión de Crisis **D1.5** Defensa Cibernética **D1.6** Redundancia de Comunicaciones
Dimensión 2 Cultura Cibernética y Sociedad (Fomentar una cultura de ciberseguridad responsable en la sociedad)	**D2.1** Mentalidad de Ciberseguridad **D2.2** Confianza y Seguridad en Internet **D2.3** Comprensión del Usuario de la Protección de Información Personal en Línea **D2.4** Mecanismos de Presentación de Informes **D2.5** Medios y Redes Sociales
Dimensión 3 Educación, Capacitación y Habilidades en Ciberseguridad (Desarrollo del conocimiento de ciberseguridad)	**D3.1** Sensibilización **D3.2** Marco para la Educación **D3.3** Marco para la Formación Profesional

Dimensión 4 Marcos Legales y Regulatorios (Creación de marcos legales y regulatorios efectivos)	**D4.1** Marcos Legales **D4.2** Sistema de Justicia Penal **D4.3** Marcos de Cooperación Formal e Informal para Combatir el Delito Cibernético
Dimensión 5 Estándares, Organizaciones y Tecnologías (Control de riesgos a través de estándares, organizaciones y tecnologías)	**D5.1** Adhesión a los Estándares **D5.2** Resiliencia de Infraestructura de Internet **D5.3** Calidad del Software **D5.4** Controles Técnicos de Seguridad **D5.5** Controles Criptográficos **D5.6** Mercado de Ciberseguridad **D5.7** Divulgación Responsable

Gráfico 2: Las cinco dimensiones del CMM

Los datos primarios utilizados en este reporte se recopilaron mediante un instrumento en línea que se distribuyó a todos los Estados Miembros de la OEA. Tras la recopilación de datos del instrumento en línea, se hizo una referencia cruzada con la investigación documental y la consulta con Estados Miembros para la validación de los resultados declarados. Utilizando el CMM como línea de base, este reporte presenta los resultados de la revisión de la capacidad de seguridad cibernética de la región de América Latina y el Caribe en base a los datos validados a diciembre de 2019. La sección de cada país concluye con una tabla resumen que presenta las cinco dimensiones y su respectivo nivel de madurez en función de los reportes de los años 2016 y 2020.

Los valores de 2016 utilizados se actualizaron para reflejar el Modelo de madurez de la capacidad de ciberseguridad para la edición revisada de las naciones (CMM). Todas las evaluaciones realizadas en la publicación de 2016 siguen siendo las mismas, excepto la inclusión de nuevos indicadores.