Unidad 4 / Escenario 7

Lectura fundamental

Ciberseguridad

Contenido

Palabras clave: ciberseguridad, ciberdefensa, cibernético, CMM, cibercultura.

El acceso a Internet ha generado un importante incremento en la productividad, la generación de empleo y los ingresos de una nación. Adicionalmente, ha permitido democratizar el acceso a la información. Sin embargo, estos beneficios se han visto altamente afectados porque las tecnologías digitales no han alcanzado el grado de madurez a nivel de seguridad, lo que conlleva a que personal con fines maliciosos se aprovechen de sus vulnerabilidades, generando unos riesgos que no solo atentan en contra de los principios de seguridad, sino que también afectan la seguridad nacional. Por lo anterior, las políticas estatales deben lograr que los países gestionen el riesgo sin perder las oportunidades que presentan las tecnologías digitales.

En este módulo estudie sobre el concepto de ciberseguridad y cómo riesgos de tecnologías digitales inmaduras afectan la seguridad de toda una nación.

1. Ciberseguridad

Según ISACA (Information Systems Audit and Control Association – Asociación de Auditoría y Control sobre los Sistemas de Información), la ciberseguridad se define como la "protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados".

En este sentido, la ciberseguridad está contenida en el estudio de seguridad de la información. La particularidad en el término de ciberseguridad es la protección a los sistemas de información digitales que se encuentran interconectados y que pueden llegar a afectar la seguridad de una nación.

La ciberseguridad debe tener un estudio especial, por lo cual la Organización de los Estados Americanos, el Banco Interamericano de Desarrollo y la Universidad de Oxford han desarrollado conjuntamente el Modelo de Madurez de Capacidad en Ciberseguridad para las Naciones, denominado en inglés Cybersecurity Capacity Maturity Model for Nations (CMM).

El CMM es una respuesta al cambio que ha tenido la era digital y la evolución de la capacidad de ciberseguridad. Para lograr esto, se han incorporado las lecciones aprendidas obtenidas del despliegue del modelo en todo el mundo y se han incluido ideas que han sido evaluadas por expertos en la materia. El CMM mantiene la estructura de la primera versión publicada en el 2015 y actualizada en el 2017, al considerar cinco dimensiones cruciales a través de las cuales se puede construir la capacidad de ciberseguridad un país (SBS, 2018):

- Política y estrategia de ciberseguridad.
- Cibercultura y sociedad.
- Educación, entrenamiento y habilidades de ciberseguridad.

- Marcos legales y regulatorios.
- Estándares, organizaciones y tecnologías.

2. Seguridad y defensa nacional

Una de las prácticas recomendadas en el Estudio de experiencias avanzadas en políticas y prácticas de ciberseguridad, realizado por el Banco Interamericano de Desarrollo en el año 2016, en el cual se presenta el panorama general en la materia para Estonia, Israel, República de Corea y Estados Unidos, concluye:

> La primera y fundamental mejor práctica para la ciberseguridad es desarrollar una estrategia nacional. Tal estrategia proporciona un marco normativo bajo el cual los países pueden organizar sus iniciativas de ciberseguridad. Su desarrollo también puede proporcionar un mecanismo que permita una amplia coordinación gubernamental transversal (Banco Interamericano de Desarrollo, 2016).

En lo referente al Estado colombiano, antes de hablar de ciberseguridad y debido al conflicto armado, ha sido necesario crear leyes de seguridad y de defensa nacional que han permitido avanzar de alguna manera en temas de ciberseguridad. La ley surgió en el año 1999 y en el 2001 quedó en firme, con reformas, actualizaciones y complementarios, como la establecida en el año 2003, que se denominó Política de Defensa y Seguridad Democrática, a continuación, las dimensiones abordadas de acuerdo con Bell Lemus (2001):

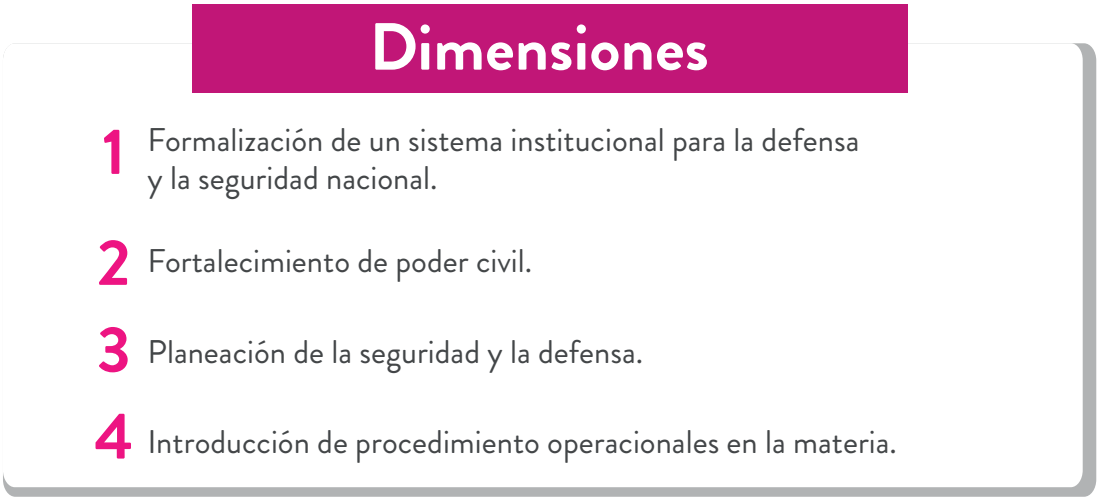

Figura 1. Dimensiones

Fuente: elaboración propia

3. Regulaciones en ciberseguridad y ciberdefensa

En el estudio referenciado anteriormente, se indica que: "La tercera mejor práctica es la adopción de leyes y normativas en materia de ciberdelincuencia, infraestructuras críticas y protección de datos. El marco jurídico y regulatorio es crucial para la ciberseguridad. Las leyes inadecuadas dificultan los esfuerzos del gobierno, perjudican a las empresas y fomentan la delincuencia informática."(Banco Interamericano de Desarrollo, 2016). Sin embargo, existen grandes diferencias entre los marcos jurídicos de los 4 países. Se ha evidenciado que cada uno cuenta con variedad de leyes existentes antes de la implementación de un modelo para ciberseguridad, al igual que de autoridades que regulan el tema.

Para el caso de Colombia, se puede identificar que existen varias normas, leyes, resoluciones, siendo las más destacadas las que se nombran en la siguiente figura:

Ley 527 de 1999

Ley sobre acceso y uso de comercio electrónico, firmas digitales y mensajes.

Decreto 1747 de 2000

Reglamentación de la Ley 527 de 1999, en lo referente a firmas digitales y entidades de certificación. Este decreto fue derogado por el art. 22, Decreto Nacional 333 de 2014.

Ley estatutaria 1266 del 31 de diciembre de 2008

Ley de hábeas data, datos personales.

Ley estatutaria 1581 de 2012

Se indican las disposiciones generales sobre la protección de datos personales. Ley de gran importancia en temas de seguridad de la información.

Decreto 1377 de 2013

Todas las leyes se reglamentan por medio de decretos. El decreto que reglamenta la ley anterior, de Datos personales es este decreto. Se indica que lo ha hecho parcialmente, puesto que debe someterse a revisión.

Ley 1341 del 30 de julio de 2009

Esta ley define los principios y conceptos sobre tecnologías de la información y comunicaciones, específicamente su organización. En esta época es creada la Agencia Nacional del Espectro.

Decreto 2573 de 2014

Como se ha mencionado, los decretos reglamentan las leyes. Para el caso de la Ley 1341, está reglamentada por el Decreto 2573. Adicionalmente, se habla de la estrategia de gobierno en línea.

Decreto Único Reglamentario del Sector TIC - Decreto 1078 del 26 de mayo de 2015

Este es un decreto especial para el sector de TICS y se ha logrado gracias al auge de las TICS, gobierno digital y economía digital. Aplica para todo el sector TICS y cobija las leyes indicadas anteriormente.

Decreto 1008 de 14 de Junio de 2018

Se establecen los lineamientos de la política de Gobierno Digital y se subroga el capítulo 1 de la parte 2 del libro 2 del Decreto 1078 de 2015.

Figura 2. Marco jurídico colombiano para la ciberseguridad
Fuente: Departamento de Planeación Nacional (2016)

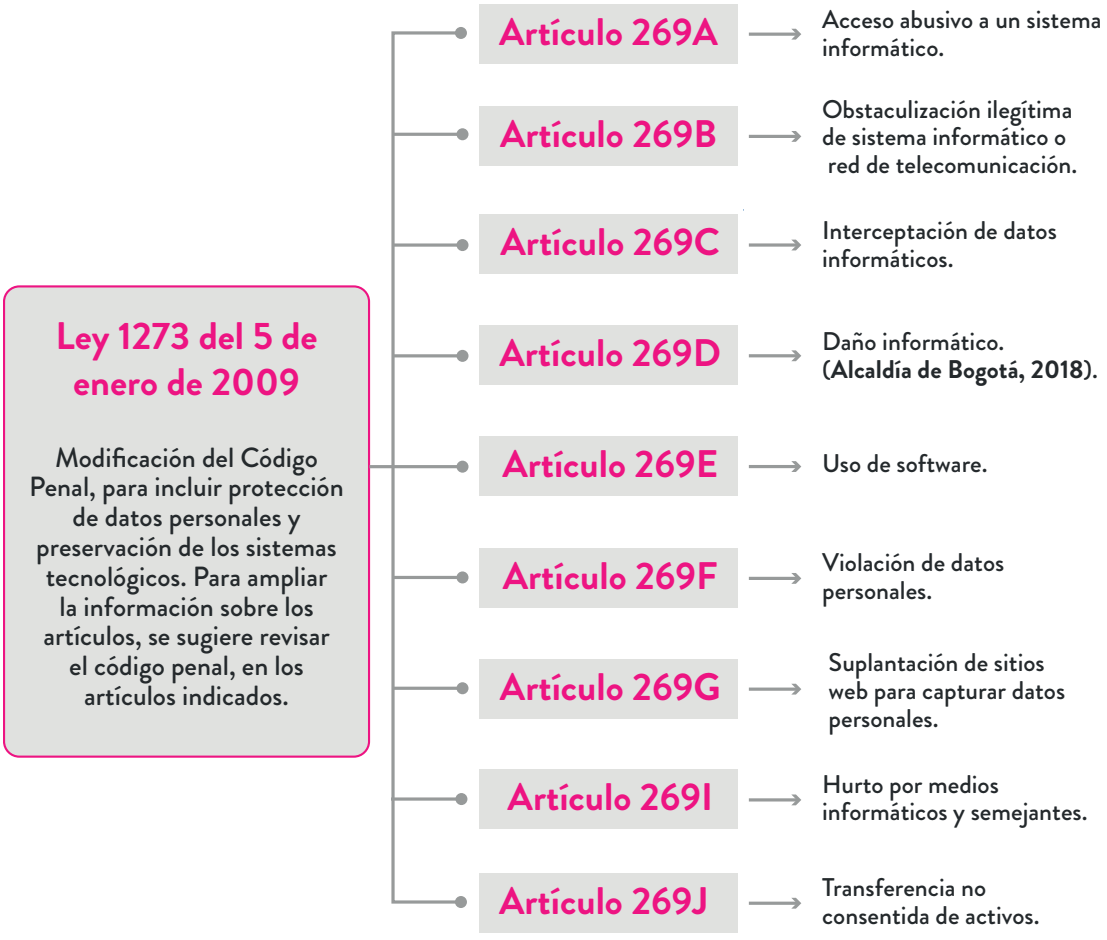

Figura 3. Ley 1273 del 5 de enero del 2009
Fuente: Departamento Nacional de Planeación. (2016)

4. Prospectiva de ciberseguridad: creación de estrategias y aplicación de modelos como herramientas claves para la ciberseguridad

4.1. Política Nacional de Seguridad Digital en Colombia

Lo más reciente en materias de ciberseguridad, específicamente en seguridad digital, es el documento CONPES: CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL REPÚBLICA DE COLOMBIA DEPARTAMENTO NACIONAL DE PLANEACIÓN POLÍTICA NACIONAL DE SEGURIDAD DIGITAL, elaborado conjuntamente por el Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Defensa Nacional —Dirección Nacional de Inteligencia— y el Departamento Nacional de Planeación en el año 2016.

El resumen ejecutivo de dicho documento se presenta a continuación:

> El creciente uso del entorno digital en Colombia para desarrollar actividades económicas y sociales, acarrea incertidumbres y riesgos inherentes de seguridad digital que deben ser gestionados permanentemente. No hacerlo, puede resultar en la materialización de amenazas o ataques cibernéticos, generando efectos no deseados de tipo económico o social para el país, y afectando la integridad de los ciudadanos en este entorno (Departamento Nacional de Planeación, 2016).

El documento analiza que el enfoque en materia de ciberseguridad se ha preocupado por fortalecer dos aspectos esenciales: defensa nacional y lucha contra el crimen. Es de resaltar que dicha perspectiva le ha permitido al país ser uno de los líderes regionales. Sin embargo, la revisión que ha hecho el país frente a su efectividad para contrarrestar los crímenes cibernéticos ha demostrado que el incremento en el uso de las TICS para realizar actividades con responsabilidad social, por ejemplo, ha generado vulnerabilidades que requieren atención desde la prevención y no solo desde la reacción. En consecuencia, la Política Nacional De Seguridad Digital ha cambiado su enfoque para incluir la gestión de riesgos como uno de los elementos más importantes para trabajar en lo referente a la seguridad digital (SBS, s.f.).

Para elegir el enfoque de la política nacional, se ha tomado como referencia a la OCDE, Organización para la Cooperación y el Desarrollo Económico, que recomienda, en el ámbito de la seguridad digital, dos cosas:

1. Implementar un conjunto de principios en todos los niveles del Gobierno y de las organizaciones públicas: estos principios suelen ser de dos tipos, generales y operativos.
    - Generales: son dirigidos a diferentes partes interesadas, quienes utilizan el entorno digital para sus actividades sociales y económicas.
    - Operativos: son dirigidos a directivos, responsables de toma de decisiones y, por tanto, encargados directos de la adopción del marco general de gestión de riesgo de seguridad nacional (SBS, 2018).
2. Adoptar una estrategia nacional para la gestión de riesgos de seguridad digital (OCDE, 2018).

La OCDE propone los principios indicados en la siguiente tabla:

Tabla 1. Principios de seguridad digital nacional OCDE

Tipo	Principio
General	Conocimiento, capacidades y empoderamiento
	Responsabilidad
	Derechos humanos y valores fundamentales
	Cooperación
Operativo	Evaluación de riesgos y ciclo de tratamiento
	Medidas de seguridad
	Innovación
	Preparación y continuidad

Fuente: elaboración propia

En lo referente a la estrategia nacional de seguridad digital, la OCDE informa que debe ser "flexible, ágil y sistémica", con el fin de alcanzar los beneficios sociales y económicos planteados; debe existir una consistencia real con los principios definidos e involucrar a las partes interesadas con un ambiente propicio para la gestión de la seguridad digital de sus actividades tanto sociales como económicas.

En la Figura 4 se puede observar el modelo resumido propuesto por la OCDE (2015) como se cita en el Documento CONPES 3854 (2016):

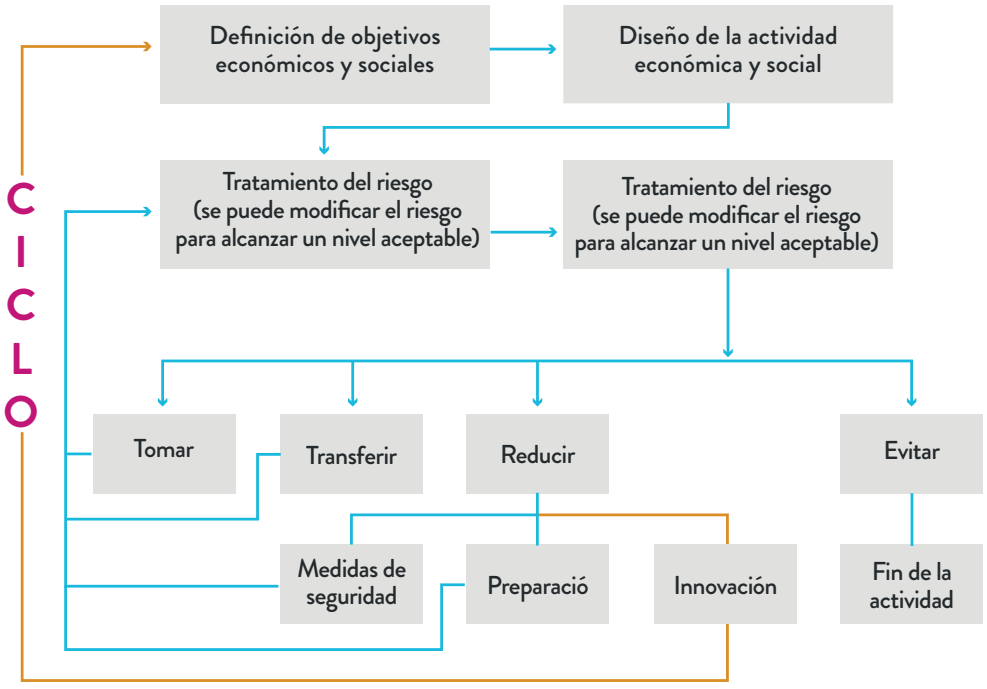

Figura 4. Modelo de gestión sistémica y cíclica del riesgo digital

Fuente: elaboración propia

En lo referente a Colombia, la Política Nacional de Seguridad Digital ha definido principios y dimensiones "con el fin de adoptar un enfoque multidimensional que garantice la seguridad digital nacional y atienda las necesidades de las partes interesadas" (Departamento Nacional de Planeación, 2016). Los principios rigen la política nacional de seguridad digital y las dimensiones son los campos de acción de esta (ver Figura 5).

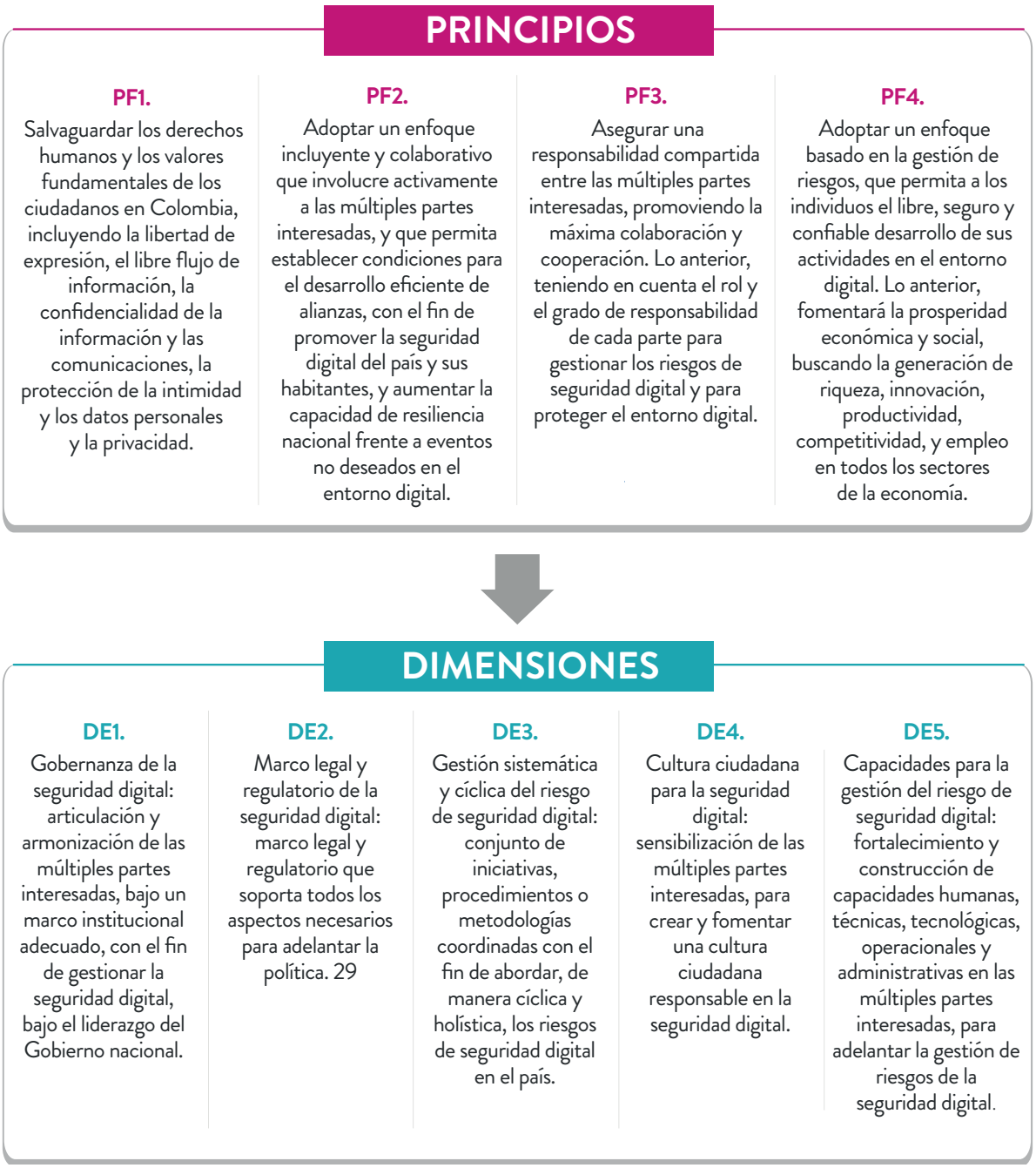

Figura 5. Principios y dimensiones de la Política Nacional de Seguridad Digital en Colombia

Fuente: elaboración propia

La Política Nacional de Seguridad digital define los siguientes conceptos para dar claridad al modelo:

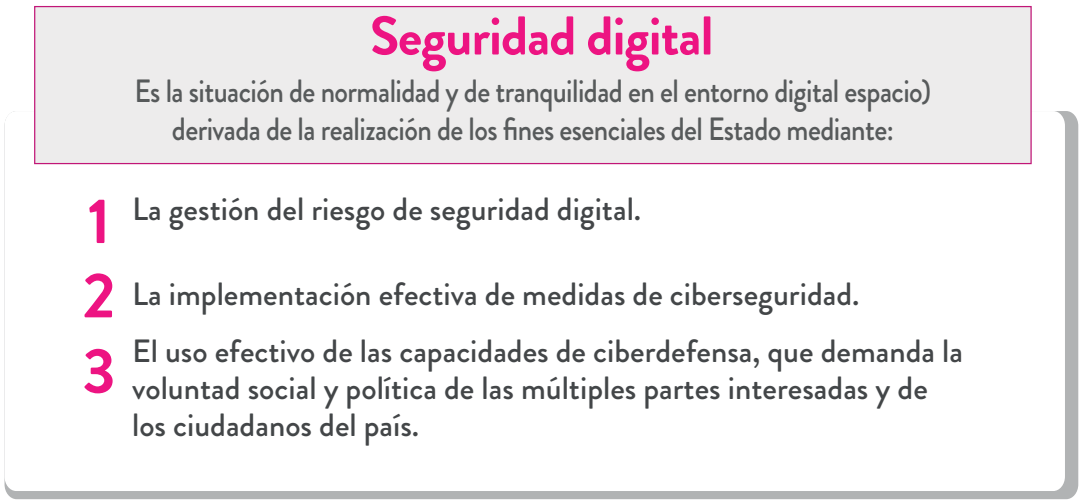

Figura 6. Seguridad digital

Fuente: elaboración propia. Modificado de Departamento Nacional de Planeación (2016)

Existen múltiples partes interesadas en la seguridad digital: el Gobierno Nacional, autoridades territoriales, las organizaciones públicas y privadas, la Fuerza Pública, los operadores de las infraestructuras críticas cibernéticas nacionales, la academia y la sociedad civil. Todos ellos dependen del entorno digital para sus actividades económicas y sociales, ejercen distintos roles y tienen diferentes responsabilidades (Departamento Nacional de Planeación 2016).

Ahora, teniendo en cuenta el documento CONPES, la infraestructura crítica cibernética nacional es aquella soportada por las TIC y por las tecnologías de operación; su funcionamiento es indispensable para la prestación de servicios para los ciudadanos y para el Estado.

La economía digital está "basada en el uso de tecnologías, cuyo desarrollo y despliegue se produce en un ecosistema caracterizado por la creciente y acelerada convergencia entre diversas tecnologías, que se concreta en redes de comunicación, equipos de hardware, servicios de procesamiento y tecnologías web" (Departamento Nacional de Planeación, 2016).

La Política De Seguridad Nacional tiene una vigencia entre el año 2016 a 2019 y se pone en marcha con su respectivo plan de acción. La inversión ha sido importante y el gobierno colombiano ha manifestado un profundo interés por cumplir a cabalidad dicho plan de acción. Las entidades con mayor grado de participación en él son Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Defensa Nacional, la Dirección Nacional de Inteligencia y el Departamento Nacional de Planeación (Departamento Nacional de Planeación, 2016).

Como se puede apreciar, el enfoque para el tema de ciberseguridad y ciberdefensa para el gobierno colombiano es el de la gestión de riesgos, sin desconocer las leyes, decretos y resoluciones que se han establecido anteriormente, pero a las cuales les ha faltado una estrategia definida en aspectos tales como la gestión de riesgos, cumplimiento de la normatividad por parte de todos los actores de la sociedad y conocimiento del ciudadano sobre dichas normativas. Como lo menciona el estudio sobre experiencias avanzadas en política y prácticas de ciberseguridad:

> La estrategia, la organización y las reglas son la primera prioridad. Una de las lecciones que puede extraerse de la experiencia de los cuatro países de referencia es que es mejor tomar medidas inmediatas antes que esperar a tener la estrategia perfecta o la ley perfecta, pues no hay estrategias perfectas. Las organizaciones siguen evolucionando según su experiencia y aprovechando las mejores prácticas de otros países. El historial de cada país muestra que la repetición y la evolución son parte de los esfuerzos nacionales para mejorar la ciberseguridad. La estrategia ha de considerarse como el inicio de un proceso que conducirá a una mejor ciberseguridad y no al fin del debate (Banco Interamericano de Desarrollo, 2016).

4.1. Modelo de Madurez de Capacidad en Ciberseguridad para las Naciones (CMM)

El Global Cyber Security Capacity Centre (GCSCC) es un centro internacional líder en la investigación sobre creación de capacidad de ciberseguridad. Apoyado por el gobierno del Reino Unido, ha creado un modelo de madurez de capacidad en ciberseguridad cuyo objetivo es aumentar la eficiencia en la creación de capacidades para los gobiernos, comunidades y organizaciones en lo referente a ciberseguridad. Al ayudar a aumentar la capacidad nacional de ciberseguridad, el centro de capacidad espera ayudar a promover un ciberespacio innovador en apoyo del bienestar, los derechos humanos y la prosperidad para todos (GCSCC, 2016).

La estructura del modelo se encuentra definida por dimensiones, factores, aspectos, estados e indicadores. En la siguiente figura se presenta la relación de estas variables; adicional, solo un ejemplo de los factores por una dimensión y los aspectos por cada uno de los factores considerados.

Figura 7. Estructura general del modelo CMM

Fuente: CGSCC (2016)

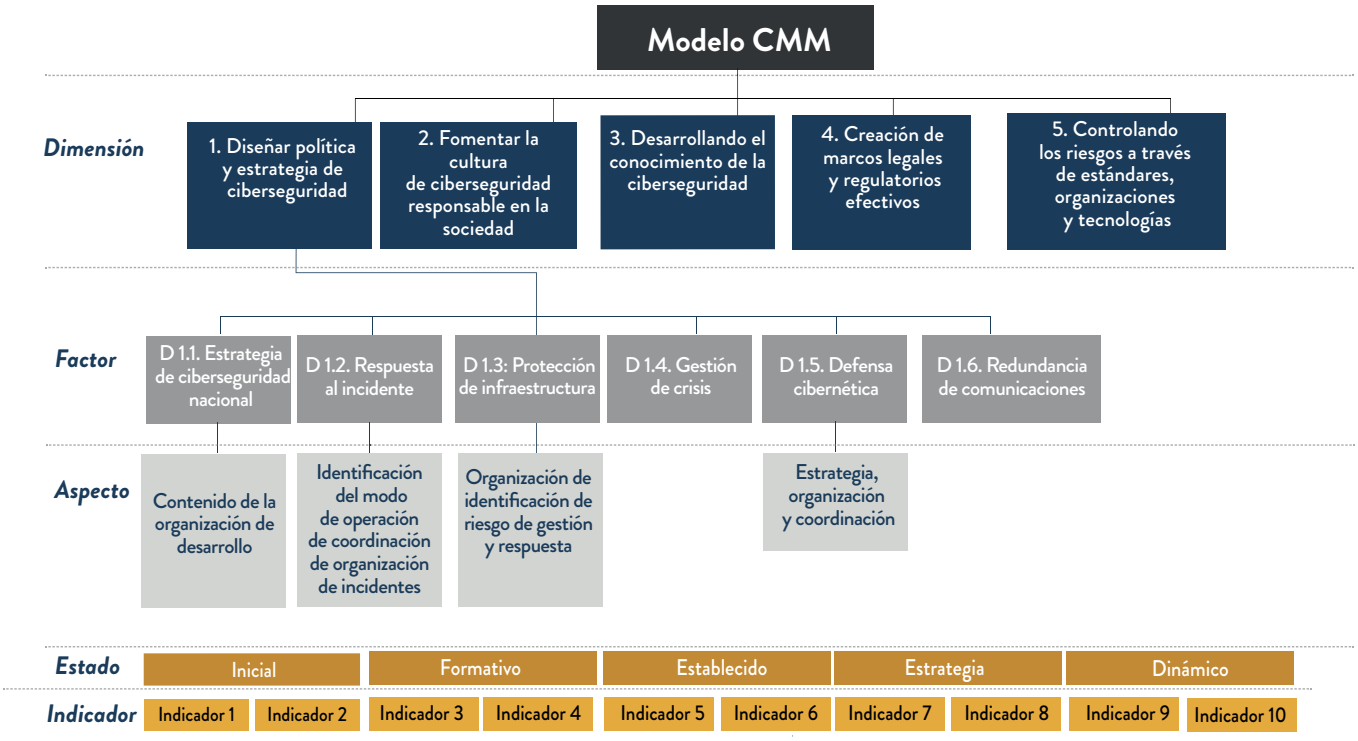

Figura 8. Ejemplo de distribución de la estructura general del modelo CMM

Fuente: elaboración propia

Para implementar el modelo, el documento que lo describe sugiere realizar una serie de tablas por cada una de las dimensiones en la cual se describa cada uno de los indicadores a cumplir. Las tablas se encuentran en *Cybersecurity Capacity Maturity Model for Nations* (CMM) (GCSCC, 2016).

5. Cuál es el reto en torno a la seguridad con estos referentes: CONPES y el modelo CMM

Para los responsables de seguridad de la información, es importante estudiar estos documentos a profundidad para que los ciudadanos del común se involucren realmente en los temas de seguridad digital.

Se ha hecho énfasis en el desarrollo de capacidades, por estar demostrado que es un elemento diferenciador en la era digital y en la transformación digital.

A nivel de ciberseguridad se identifican dimensiones que complementan el documento CONPES en lo referente a una política de seguridad de la información orientada al análisis de riesgos. Para comprender mejor la relación entre las dimensiones del modelo CMM y CONPES, se realiza la siguiente asociación:

Tabla 2. Asociación dimensiones del modelo CMM y CONPES

Política y estrategia de ciberseguridad	⇒	DE1 Gobernanza de seguridad digital
Marcos legales y regulatorios	⇒	DE2 Marco legal y regulatorio
Estándares, organizaciones y tecnología	⇒	DE3 Gestión sistémica y cíclica del riesgo de seguridad digital
Educación, entrenamiento y habilidades de ciberseguridad	⇒	DE4: Cultura ciudadana para la seguridad digital
Cibercultura y sociedad	⇒	DE5: Capacidades para la gestión del riesgo de seguridad digital

Fuente: Politécnico Grancolombiano

Por tal motivo, la mejor manera para validar el cumplimiento del gobierno colombiano es tomar como referente uno de los países que ha adoptado el modelo y comprender los indicadores de cada una de las dimensiones, con el fin de contar con información comparativa de un modelo de aplicación mundial con respecto a lo definido en el documento CONPES.

Este ejercicio puede resultar algo ambicioso, puesto que se requieren datos de todas las entidades públicas en Colombia. Sin embargo, se facilita con el uso del mecanismo de Datos Abiertos, ofrecidos por el Gobierno Nacional.

Datos Abiertos es el recurso que utilizan las entidades públicas para indicarle a la ciudadanía los resultados de su gestión y que deben cumplir la normativa de gestión documental definida por el Gobierno.

Otra manera de revisar las estadísticas es considerar el estudio realizado por el Banco Internacional de Desarrollo llamado *Experiencias avanzadas en políticas y prácticas de Ciberseguridad. América Latina y el Caribe*; este es del año 2016, por lo cual se espera que en el presente año pueda salir un nuevo estudio. Esta investigación puede ser comparada con el documento *Experiencias avanzadas en políticas y prácticas de ciberseguridad*, en el cual se muestran los resultados de Estonia, Israel, República de Corea y Estados Unidos en cuanto a los temas de ciberseguridad, describe cada dimensión y lo que hace cada país para cumplir un nivel específico por cada una de ellas.

De la revisión de los dos documentos indicados, se puede identificar que el documento CONPES ha aportado en temas de estrategia y, por tanto, Colombia, en muchos factores evaluados por el modelo, alcanza un nivel "Establecido". Sin embargo, comparado con países como Estados Unidos, la política de ciberseguridad se encuentra poco avanzada, como es el caso de planes de respuesta o continuidad de negocio.

Este tipo de análisis nos muestra que el verdadero reto a nivel de ciberseguridad es cumplir las reglas que el Estado define y eso implica participar activamente en la revisión de los documentos que se emiten, analizar los datos de fuentes externas, comprender las prácticas de otras naciones, para replicarlas y estructurar el tema de seguridad en el desarrollo de capacidades y evaluación por madurez.

Referencias

Banco Interamericano de Desarrollo. (2016). *Experiencias avanzadas en políticas y prácticas de Ciberseguridad.Panorama general de Estonia, Israel, República de Corea y Estados Unidos:* Recuperado de https://publications.iadb.org/bitstream/handle/11319/7759/Experiencias-avanzadas-en-politicas-y-practicas-de-ciberseguridad-Panorama-general-de-Estonia-Israel-Republica-de-Corea-y-Estados-Unidos.pdf?sequence=7

Bell Lemus, G. B. (21 de Agosto de 2001). *Qué es la ley de defensa y seguridad nacional.* El Tiempo. Recuperado de http://www.eltiempo.com/archivo/documento/MAM-466426

Congreso de Colombia. (18 de agosto de 1999). *Ley 527 de 1999. DO: 43.673 del 21 de Agosto de 1999*. Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276

Congreso de Colombia (31 de diciembre de 2008). *Ley 1266 de 2008. DO: 47.219 de diciembre 31 de 2008*. Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488

Congreso de Colombia (5 de enero de 2009). *Ley 1273 de 2009. DO: 47.223 de enero 5 de 2009.* Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

Congreso de Colombia (17 de octubre de 2012). *Ley 1581 de 2012.* Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

Congreso de Colombia (11 de septiembre de 2000). *Decreto 1747 de 2000*. Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4277

Departamento Nacional de Planeación. (2016). *Política Nacional de Seguridad Digital.* Bogotá, Colombia: CONPES. Recuperado de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

GCSCC. (2016). *Cybersecurity Capacity Maturity Model for Nations (CMM)*. Recuperado de https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cybersecurity-capacity-maturity-model-nations-cmm-0

OCDE. (2018). *Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity in Digital Security Risk Management for Economic and Social Prosperity, OCDE Recommendation and Companion Document.* Paris, Francia: OCDE Publishing. Recuperado de http://www.OCDE.org/sti/ieconomy/digital-security-risk-management.pdf

Oxford Martin School (s.f.). *Global Cyber Security Capacity Centre.* Recuperado de https://www.oxfordmartin.ox.ac.uk/cybersecurity/

SBS. (s.f.). *Cybersecurity Capacity Portal.* Recuperado de https://www.sbs.ox.ac.uk/cybersecurity-capacity.

Referencias de imágenes

CGSCC. (2016). E*structura general del modelo CMM* [Figura]. Recuperado de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Departamento Nacional de Planeación. (2016). *Marco jurídico colombiano para la ciberseguridad* [Figura]. Recuperado de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Departamento Nacional de Planeación. (2016). *Ley 1273 del 5 de enero del 2009* [Figura]. Recuperado de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

INFORMACIÓN TÉCNICA

FACULTAD DE
INGENIERÍA, DISEÑO
E INNOVACIÓN

Módulo: Teoría de la Seguridad

Unidad 4: Seguridad en la nuevas tendencias de TI

Escenario 7: Ciberseguridad

Autor: Alexandra Peña Daza

Asesor Pedagógico: Angie Viviana Laitón Fandiño

Diseñador Gráfico: Henderson Jhoan Colmenares

Asistente: Alejandra Morales