GUÍA PARA LA ELABORACIÓN DE UNA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

PARTICIPACIÓN ESTRATÉGICA EN LA CIBERSEGURIDAD

ITU
CCDCOE
The Commonwealth Cybercrime Initiative
CTO
THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP
Deloitte.
Global Cyber Security Capacity Centre
GCSP
Microsoft

Ciertos Derechos Reservados

Derechos y Permisos

(UIT), el Banco Mundial, la Secretaría de la Commonwealth (Comsec), la Organización de Telecomunicaciones de la Commonwealth (CTO) y el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCDCOE OTAN). *Los puntos de vista y opiniones expresados en la adaptación son responsabilidad exclusiva del autor o autores de la adaptación y no están avalados por las organizaciones antes mencionadas.*

Contenido de terceros: La Unión Internacional de Telecomunicaciones (UIT), el Banco Mundial, la Secretaría de la Commonwealth (Comsec), la Organización de Telecomunicaciones de la Commonwealth (CTO) y el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCDCOE OTAN) no son necesariamente propietarios de cada una de las partes del contenido de esta obra. Por lo tanto, no se garantiza que la utilización de cualquier componente o parte individual propiedad de terceros contenida en la obra no infrinja los derechos de dichos terceros. El riesgo de querella que resulte de tal infracción recae únicamente en usted. Si desea reutilizar un componente de la obra, es su responsabilidad determinar si necesita permiso para esa reutilización y obtener el eventual permiso del propietario de los derechos de autor. Ejemplos de componentes son, entre otros, cuadros, figuras o imágenes.

Toda solicitud de utilización que transcienda el ámbito de aplicación de este tipo de licencia (CC BY 3.0 IGO) deberá dirigirse a la Unión Internacional de Telecomunicaciones (UIT), Place des Nations, 1211 Ginebra 20, Suiza; correo electrónico: itumail@itu.int.

Agradecimientos

Esta guía ha sido elaborada por 12 asociados de organizaciones intergubernamentales e internacionales, del sector privado, así como del mundo académico y de la sociedad civil, concretamente las siguientes organizaciones: Secretaría del Commonwealth (Comsec), Organización de Telecomunicaciones del Commonwealth (CTO), Deloitte, Centro de Política de Seguridad de Ginebra (GCSP), Centro Global de Capacitación en Ciberseguridad (GCSCC) de la Universidad de Oxford, Unión Internacional de Telecomunicaciones (UIT), Microsoft, Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCDCOE OTAN), Instituto Potomac de Estudios Políticos, RAND Europa, Banco Mundial y Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD).

El equipo estaba integrado por Katalaina Sapolu (Comsec), Shadrach Haruna (Comsec), Martin Koyabe (CTO), Fargani Tambeayuk (CTO), Andrea Rigoni (Deloitte), Carolin Weisser (GCSCC), Marco Obiso (UIT), Kaja Ciglic (Microsoft), Kadri Kaska (CCDCOE OTAN), Francesca Spidalieri y Melissa Hathaway (Instituto Potomac de Estudios Políticos), Erik Silfversten (RAND Europa), David Satola y Sandra Sergeant (Banco Mundial) y Cecile Barayre (UNCTAD).

La Agencia Europea de Seguridad de las Redes y de la Información (ENISA) aportó una importante contribución a la guía.

También se reconoce la contribución de las siguientes personas: Grace Acayo, Rosheen AwotarMauree, Ben Baseley-Walker, Paul Cornish, Luc Dandurand, Michael Goldsmith, Kemal Huseinovic, Andraz Andy Kastelic, Maxim Kushtuev, Lena Lattion, Gustav Lindstrom, Damien Maddalena, Emily Munro, Lara Pace, Sarah Puello Alfonso, Valeria Risuglia, Taylor Roberts, Monica M. Ruiz, Irene Rubio, Ann Valjataga, Julienne Wright.

Prólogo

Me complace presentar, en nombre de todos los asociados, la presente guía sobre la elaboración de estrategias nacionales de ciberseguridad, destinada a proporcionar una recopilación armonizada de principios y buenas prácticas acerca de la elaboración, establecimiento y aplicación de estrategias nacionales de ciberseguridad.

Propiciado por la UIT, 12 asociados de los sectores público y privado, del mundo académico y de la sociedad civil acordaron compartir sus experiencias, conocimientos y pericia con el fin de elaborar esta guía que reúne los conocimientos prácticos de las organizaciones participantes, así como referencias a publicaciones complementarias, con objeto de facilitar el acceso a los recursos disponibles.

En los dos últimos decenios, miles de millones de personas de todo el mundo se han beneficiado del crecimiento exponencial y la rápida adopción de las tecnologías de la información y la comunicación, así como de las oportunidades económicas y sociales conexas. Estamos asistiendo a una revolución digital que transforma profundamente nuestras sociedades.

La ciberseguridad es un factor fundamental para lograr el desarrollo socioeconómico. Sin embargo, sólo 76[1] países del mundo cuentan con estrategias nacionales de ciberseguridad disponibles públicamente. Por lo tanto, es imperativo redoblar los esfuerzos para su elaboración. Como su título indica, el objetivo de la guía es fomentar el pensamiento estratégico y ayudar a los dirigentes y los poderes públicos nacionales a elaborar, establecer y aplicar estrategias nacionales de ciberseguridad.

Confío en que la guía para la elaboración de estrategias nacionales de ciberseguridad constituya un instrumento útil para todas las partes interesadas con responsabilidades en materia de ciberseguridad. Quisiera manifestar personalmente mi gratitud a los asociados por su continuo e inestimable apoyo y compromiso para hacer de este proyecto un gran éxito, que constituye un ejemplo real de colaboración multipartita.

Brahima Sanou
Director de la Oficina de Desarrollo de las Telecomunicaciones de la UIT

[1] Según el índice de ciberseguridad mundial (GCI) 2017 de la UIT.

Índice

Prefacio

La presente guía para la elaboración de estrategias nacionales de ciberseguridad ofrece una de las panorámicas más completas de lo que constituyen estrategias de ciberseguridad exitosas. Es el resultado de un esfuerzo multipartito único, colaborativo y equitativo, que aprovecha los conocimientos, la experiencia y la pericia de muchas organizaciones en el ámbito de las estrategias y políticas nacionales en materia de ciberseguridad. Concretamente, esta guía ha sido elaborada por 12 asociados de los sectores público y privado, así como del mundo académico y de la sociedad civil.

Los asociados reconocieron la necesidad de reforzar la cooperación y la coordinación entre la comunidad internacional en materia de capacitación en ciberseguridad. Este esfuerzo colaborativo tiene por objeto ayudar a los dirigentes y a los poderes públicos nacionales a elaborar respuestas defensivas a las ciberamenazas, en la forma de una estrategia nacional de ciberseguridad, y a pensar estratégicamente acerca de la ciberseguridad, la preparación cibernética, la respuesta y la resiliencia, creando así confianza y seguridad en las tecnologías de la información y la comunicación (TIC).

La guía de estrategias nacionales de ciberseguridad ha sido elaborada siguiendo un método iterativo, con el que se pretendía llegar a un acuerdo mediante la creación de consenso. Se basa en los recursos existentes y tiene por objeto facilitar su utilización por las partes interesadas nacionales. En la medida de lo posible, las fuentes e instrumentos pertinentes utilizados para elaborar cada conjunto de recomendaciones se enumeran en la sección de referencias a fin de fomentar su uso más amplio.

La ciberseguridad es un aspecto fundamental para la consecución de los objetivos socioeconómicos de las economías modernas. Se espera que esta guía sobre estrategias nacionales de ciberseguridad pueda servir de instrumento útil para todas las partes interesadas, incluidos los poderes públicos, los legisladores y los reguladores nacionales, que tienen responsabilidades en el ámbito de la ciberseguridad. Además, podría tener más aplicaciones, ya que los conceptos explicados pueden aplicarse a nivel regional o municipal y también adaptarse para el sector privado.

1 Descripción general del documento

1.1 Finalidad

La finalidad del presente documento es orientar a los dirigentes y poderes públicos nacionales en la elaboración de una estrategia nacional de ciberseguridad y en la reflexión estratégica sobre la ciberseguridad, la preparación para el ciberespacio y la resiliencia.

Esta guía tiene por objeto proporcionar un marco útil, flexible y fácil de utilizar para establecer el contexto de la visión socioeconómica del país y su actual postura en materia de seguridad, así como ayudar a los poderes públicos a elaborar una estrategia que tenga en cuenta la situación particular del país y sus valores culturales y sociales, y que fomente la creación de sociedades seguras, resilientes, basadas en las TIC y conectadas.

Esta guía es un recurso sin precedentes, por cuanto proporciona un marco que ha sido acordado por organizaciones con experiencia demostrada y diversa en esta esfera temática y que se basa en sus trabajos previos en este campo. Así, ofrece la visión general más exhaustiva disponible hasta la fecha de lo que constituyen las estrategias nacionales de ciberseguridad que han tenido éxito.

1.2 Ámbito de aplicación

La ciberseguridad constituye un reto complejo que comprende diversos aspectos de gobernanza, políticos, operativos, técnicos y jurídicos. La presente guía trata de abordar, organizar y priorizar muchos de estos aspectos recurriendo a modelos, marcos y otras referencias existentes y bien reconocidos.

La guía se concentra en la protección de los aspectos civiles del ciberespacio y, por tanto, destaca los principios generales y las buenas prácticas que deben tenerse en cuenta al preparar, elaborar y gestionar toda estrategia nacional de ciberseguridad.

A tal efecto, la guía establece una clara distinción entre el “proceso” que adoptarán los países durante el ciclo de vida de una estrategia nacional de ciberseguridad (iniciación, inventario y análisis, producción, aplicación y revisión) y el “contenido”, es decir, el texto propiamente dicho que figurará en el documento donde se defina la estrategia nacional de ciberseguridad. La guía no abarca aspectos tales como el desarrollo de cibercapacidades defensivas u ofensivas por parte de las fuerzas militares, las fuerzas de defensa o los organismos de inteligencia de un país, si bien varios países han estado desarrollando esas capacidades.

A fin de dar orientaciones y buenas prácticas acerca de "qué" debe incluirse en una estrategia nacional de ciberseguridad, así como de "cómo" se debe elaborar, aplicar y revisar, en la presente guía se tratan ambos aspectos.

La guía también ofrece un panorama general de los componentes básicos que necesita un país para estar ciberpreparado, destacando los aspectos cruciales que los gobiernos deben tener en cuenta al elaborar sus estrategias y planes de ejecución nacionales.

Por último, esta guía ofrece a los poderes públicos una visión global y general de alto nivel de los planteamientos y aplicaciones existentes, así como referencias a recursos adicionales y complementarios que pueden servir de base para las iniciativas nacionales específicas en materia de ciberseguridad.

1.3 Estructura general y utilización de la guía

Esta guía se ha estructurado principalmente como un recurso para ayudar a los actores gubernamentales en la preparación, redacción y gestión de su estrategia nacional de ciberseguridad. El contenido se ha organizado de modo que siga el proceso y el orden de desarrollo de una estrategia:

- Sección 2 – Introducción: presenta una descripción general del tema de la guía con las correspondientes definiciones.
- Sección 3 – Ciclo de elaboración de la estrategia: detalla las etapas de la elaboración de la estrategia y su gestión durante todo su ciclo de vida.
- Sección 4 – Principios generales de la estrategia: esboza las consideraciones intersectoriales y fundamentales que deben tenerse en cuenta durante la elaboración de una estrategia.
- Sección 5 – Esferas prioritarias y buenas prácticas: identifica los temas y aspectos fundamentales que se han de considerar al elaborar la estrategia.
- Sección 6 – Materiales de referencia de apoyo: se remite a otras fuentes relevantes que las partes interesadas pueden examinar durante el proceso de elaboración.

En particular, en la sección 3 se abordan el proceso y los aspectos relacionados con la elaboración de una estrategia nacional de ciberseguridad (como la preparación, la redacción, la aplicación y la sostenibilidad a largo plazo), mientras que las secciones 4 y 5 se centran más en el contenido de la estrategia nacional de ciberseguridad, ya que ponen de relieve los conceptos y elementos que debe contener el documento.

1.4 Destinatarios

La presente guía está destinada ante todo a los poderes públicos encargados de elaborar una estrategia nacional de ciberseguridad. Los destinatarios secundarios son todos los demás agentes públicos y privados que participan en la elaboración y aplicación de una estrategia, como los funcionarios responsables, las autoridades reguladoras, las fuerzas de seguridad, los proveedores de TIC, los operadores de infraestructura esencial, la sociedad civil, las instituciones académicas y los institutos de investigación. La guía también podría resultar útil para los diferentes agentes de la comunidad internacional de desarrollo que prestan asistencia en materia de ciberseguridad.

2 Introducción

En los dos últimos decenios, miles de millones de personas de todo el mundo se han beneficiado del crecimiento exponencial y la rápida adopción de las tecnologías de la información y la comunicación, así como de las oportunidades económicas y sociales conexas.

Desde su creación, Internet ha evolucionado desde una plataforma de intercambio de información hasta convertirse en la columna vertebral de los negocios modernos, los servicios e infraestructuras esenciales, las redes sociales y la economía global en su conjunto. En consecuencia, los dirigentes nacionales han comenzado a poner en marcha estrategias digitales y a financiar proyectos que aumenten la conectividad a Internet y aprovechen los beneficios derivados de la utilización de las TIC, con el fin de estimular el crecimiento económico, aumentar la productividad y la eficiencia, mejorar la prestación de servicios y su capacidad, proporcionar acceso a los negocios y a la información, permitir el aprendizaje electrónico, mejorar las aptitudes de la población activa y promover la buena gobernanza. Los países no pueden hacer caso omiso de las oportunidades que conlleva estar conectado y participar en la economía de Internet.

Si bien la dependencia de nuestras sociedades de la infraestructura digital no deja de aumentar, la tecnología sigue siendo intrínsecamente vulnerable. La confidencialidad, la integridad y la disponibilidad de la infraestructura de las TIC se ven amenazadas por la rápida evolución de las ciberamenazas, como el fraude electrónico, el robo de la propiedad intelectual y de la información de identificación personal, la interrupción de los servicios y los daños o la destrucción de la propiedad. El poder transformador de las TIC y de Internet en cuanto catalizadores del crecimiento económico y del desarrollo social se encuentra en un punto crítico en el que la confianza y fe de los ciudadanos y de los países en la utilización de las TIC está siendo menoscabada por la inseguridad cibernética.

Para aprovechar plenamente el potencial de la tecnología, los Estados deben armonizar sus visiones económicas nacionales con sus prioridades de seguridad nacional. Si los riesgos para la seguridad debidos a la proliferación de infraestructura de TIC y aplicaciones de Internet no se equilibran adecuadamente con exhaustivas estrategias nacionales de ciberseguridad y planes de resiliencia, los países no podrán alcanzar el crecimiento económico y los objetivos de seguridad nacional que persiguen.

En consecuencia, los países están desarrollando capacidades tanto ofensivas como defensivas para contrarrestar las actividades ilícitas e ilegales en el ciberespacio y para prevenir incidentes antes de que causen daños a sus naciones. En este

documento se analizan específicamente las respuestas defensivas, en particular en forma de estrategias nacionales de ciberseguridad.

Mediante el desarrollo y la aplicación de una estrategia nacional de ciberseguridad, los países pueden mejorar la seguridad de su infraestructura digital y, en última instancia, contribuir a sus aspiraciones socioeconómicas más amplias. Los líderes nacionales deben adoptar una actitud estratégica en cuanto a las oportunidades que ofrece el entorno digital y los riesgos que entraña para sus países; también deben tener una clara visión del futuro digital que desean crear.

2.1 Qué es la ciberseguridad

Existen varias definiciones del término "ciberseguridad" a escala nacional e internacional. A los efectos del presente documento, por "ciberseguridad" se entiende el conjunto de herramientas, políticas, directrices, métodos de gestión de riesgos, acciones, formaciones, prácticas idóneas, garantías y tecnologías que pueden utilizarse para proteger la disponibilidad, integridad y confidencialidad de los activos de la infraestructura conectada pertenecientes al gobierno, a las organizaciones privadas y a los ciudadanos; estos activos incluyen los dispositivos informáticos conectados, el personal, la infraestructura, las aplicaciones, los servicios, los sistemas de telecomunicaciones y los datos en el mundo cibernético[2].

2.2 Beneficios de la estrategia nacional de ciberseguridad y proceso de elaboración de la estrategia

La estrategia nacional de ciberseguridad puede adoptar muchas formas y pueden entrar en distintos niveles de detalle, dependiendo de los objetivos y niveles de preparación cibernética de cada país. Por consiguiente, no existe una definición consolidada y comúnmente acordada de lo que constituye una estrategia nacional de ciberseguridad.

Basándose en la investigación existente en este ámbito, este documento anima a las partes interesadas a considerar que la estrategia nacional de ciberseguridad es:

- una expresión de la visión, los objetivos de alto nivel, los principios y las prioridades que orientan a un país a la hora de abordar la ciberseguridad;
- una concepción general que tienen los agentes encargados de mejorar la ciberseguridad del país y de sus respectivas funciones y responsabilidades; y
- una descripción de las medidas, programas e iniciativas que un país adoptará para proteger su infraestructura cibernética nacional y, a lo largo de ese proceso, aumentar su seguridad y resiliencia.

[2] Definición adaptada de https://www.bcmpedia.org/wiki/Cyber_Security.

Establecer la visión, los objetivos y las prioridades permite a los gobiernos considerar la ciberseguridad de forma global en todo su ecosistema digital nacional, en lugar de en un determinado sector, objetivo o en respuesta a un riesgo específico, es decir, les permite ser estratégicos. Las prioridades de la estrategia nacional de ciberseguridad varían de un país a otro, por lo que, si bien un país puede concentrarse en los riesgos intrínsecos para la infraestructura, otros pueden centrarse en la protección de la propiedad intelectual, el fomento de la confianza en el mundo en línea, la mejora de la conciencia pública en general en materia de ciberseguridad o en una combinación de estos aspectos.

La necesidad de identificar y luego priorizar las inversiones y los recursos es fundamental a la hora de gestionar convenientemente los riesgos en un ámbito tan amplio como la ciberseguridad.

La estrategia nacional de ciberseguridad también ofrece la oportunidad de armonizar las prioridades en este campo con otros objetivos relacionados con las TIC. La ciberseguridad es fundamental para alcanzar los objetivos socioeconómicos de las economías modernas, razón por la cual en la estrategia se debería exponer cómo ayudar a conseguir esos objetivos. A tal efecto, se puede remitir a las políticas existentes destinadas a ejecutar los programas digitales o de desarrollo del país o evaluar cómo incorporar la ciberseguridad en ellos.

Por último, el proceso de elaboración de la estrategia nacional de ciberseguridad debe traducir la visión del gobierno en políticas coherentes y viables que le ayuden a alcanzar sus objetivos. Quedan comprendidas no sólo las medidas, los programas y las iniciativas que han de ponerse en marcha, sino también los recursos asignados a esos efectos y la forma en que deben utilizarse esos recursos. Análogamente, el proceso debe identificar las métricas que se utilizarán para velar por que los resultados deseados se logren dentro de los presupuestos y plazos establecidos.

3 Ciclo de vida de la estrategia nacional de ciberseguridad

En esta sección se describen las diversas fases de la elaboración de una estrategia, que son las siguientes:

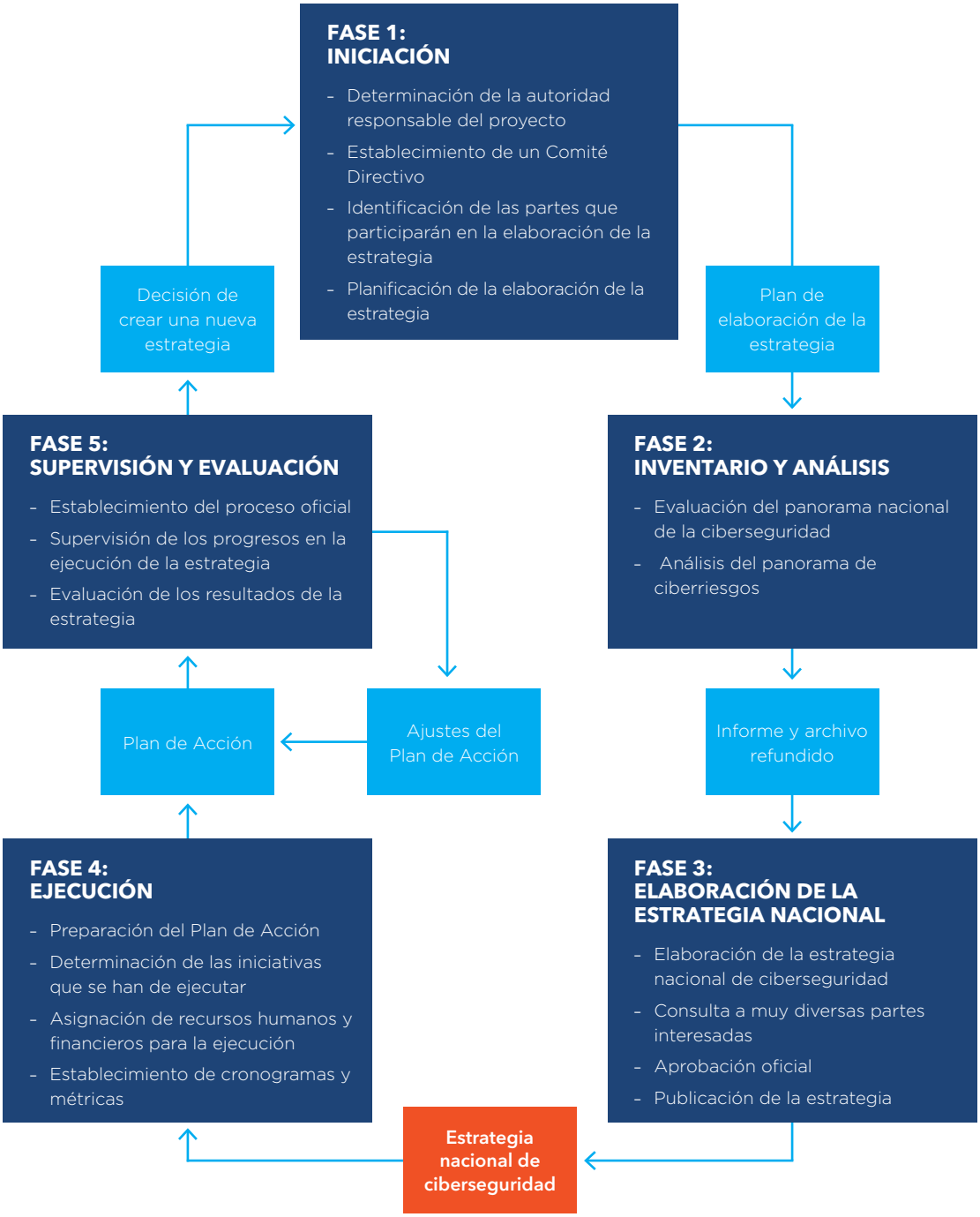
- Fase I - Iniciación
- Fase II - Inventario y análisis
- Fase III - Producción
- Fase IV - Ejecución
- Fase V - Seguimiento y evaluación

En esta sección también se presentan las principales entidades que deben participar en la elaboración de la estrategia y se destacan otras partes que podrían contribuir al proceso.

En última instancia, esta sección tiene por objeto facilitar al lector la comprensión de las etapas que debe seguir una nación para elaborar una estrategia nacional y los posibles mecanismos para su ejecución de acuerdo con sus necesidades y requisitos específicos, integrando los principios generales (descritos en la sección 4) y las buenas prácticas (descritos en la sección 5).

Este ciclo de vida, como se ilustra en la Figura 1, sirve para orientar al usuario del presente documento a concebir la ciberseguridad de un modo estratégico a escala nacional.

Figura 1 *- Ciclo de vida de la estrategia nacional de ciberseguridad*



3.1 Fase I: Iniciación

De conformidad con las secciones 4 y 5 del presente documento, la fase de iniciación de la estrategia nacional de ciberseguridad sienta las bases para su eficiente elaboración. Cabe esperar que esta fase se concentre en los procesos, los plazos y la identificación de las principales partes que deben participar en la elaboración de la estrategia. Esta fase culmina con la elaboración de un plan de preparación de la estrategia. Cuando así lo contemple el procedimiento administrativo del país, el plan puede requerir la aprobación del Ejecutivo3.

3.1.1 Identificación de la autoridad responsable del proyecto

En consonancia con el principio de definir claramente los dirigentes, las funciones y la atribución de recursos (sección 4.8), el proceso de elaboración de la estrategia debe ser coordinado por una sola autoridad competente. El Ejecutivo debe designar a una entidad pública, existente o creada a tal efecto, ya sea un ministerio, una agencia o un departamento, para que dirija la elaboración de la estrategia. Esta entidad, denominada en el presente documento como autoridad responsable del proyecto, debe, a su vez, nombrar a la persona encargada y responsable de dirigir el proceso de elaboración de la estrategia.

La autoridad responsable del proyecto debe ser neutral durante todo el proceso de elaboración. Con este fin, se recomienda que esta entidad sea diferente de la entidad o entidades que serán responsables de ejecutar la estrategia. Cabe adoptar este u otros mecanismos para salvar cualquier sesgo inherente y evitar la competencia intragubernamental por los recursos.

3.1.2 Establecimiento de un Comité Directivo

El Ejecutivo también debe establecer un Comité Directivo que colabore con la autoridad responsable del proyecto en la elaboración de la estrategia. Debe estar facultado para dar orientaciones y desempeñar un papel en el control de calidad. Además, debe garantizar la transparencia e inclusividad del proceso, de conformidad con el principio de definir claramente los dirigentes, las funciones y la atribución de recursos (sección 4.8). El papel, la estructura y la composición del Comité Directivo deben estar claramente definidos desde el principio.

Dado que el Comité Directivo tal vez necesite examinar documentos confidenciales, debe constituirse en consecuencia. También es importante que su composición se corresponda con las diversas responsabilidades asignadas a este órgano, por ejemplo, efectuando nombramientos teniendo en cuenta la antigüedad.

[3] Persona o entidad facultada para tomar decisiones a escala nacional.

3.1.3 Determinación de las partes que participarán en la elaboración de la estrategia

En esta etapa, la autoridad responsable del proyecto debe determinar un conjunto inicial de partes que participarán en la elaboración de la estrategia. También debe aclarar las funciones de cada una de las partes y esbozar la forma en que colaborarán para gestionar las expectativas a lo largo de todo el proceso.

Es posible que durante el proceso la autoridad responsable del proyecto tenga que ponerse en contacto con otras partes para asegurarse de que se emplean todos los conocimientos y experiencias pertinentes. De esta forma se aplicaría el principio de inclusividad (sección 4.3), que destaca la importancia de la cooperación con distintos agentes del gobierno, el sector privado y la sociedad civil. Por ejemplo, la autoridad responsable del proyecto podría considerar la posibilidad de incluir a empresas de TIC, operadores de infraestructura esencial, expertos del mundo académico y organizaciones no gubernamentales que colaboren, entre otras cosas, en la sensibilización y preparación en materia de ciberseguridad.

Ese mecanismo de cooperación podría adoptar la forma de un comité asesor que contribuiría aportando miembros al Comité Directivo y al que se podría consultar sobre las diversas fases.

3.1.4 Planificación de la elaboración de la estrategia

Al final de la fase inicial, la autoridad responsable del proyecto debe preparar un plan de elaboración de la estrategia nacional de ciberseguridad. Una vez redactado dicho plan, debe presentarse, según proceda, al Comité Directivo y al Ejecutivo para su aprobación, de conformidad con los procedimientos de gobernanza nacionales.

Al redactar el plan, la autoridad responsable del proyecto también debe considerar si la estrategia nacional de ciberseguridad adoptará la forma de legislación o de política, ya que cada opción podría requerir procedimientos oficiales diferentes e influir también en el calendario para su adopción.

El plan de elaboración de la estrategia debe identificar las principales etapas y actividades, las partes más importantes, los plazos y los recursos necesarios. Debe especificar cómo y cuándo se espera que las partes participen en el proceso de elaboración aportando sus contribuciones y opiniones.

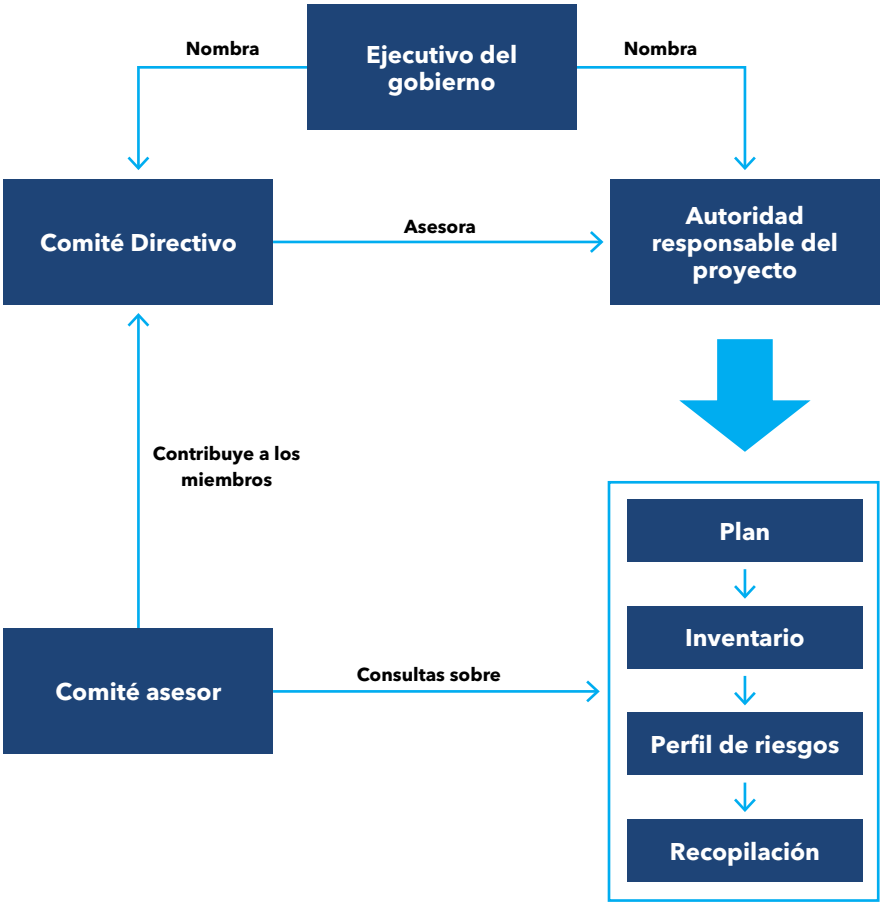
También debe identificar los recursos humanos y financieros necesarios y dónde pueden obtenerse. Por ejemplo, los conocimientos especializados necesarios podrían solicitarse a organizaciones intergubernamentales, al sector privado, al mundo académico o a organismos de desarrollo. Análogamente, la financiación necesaria podría obtenerse de la reasignación de fondos especiales en los presupuestos existentes o de nuevos fondos disponibles de terceros (por ejemplo, organizaciones internacionales).

Debe prestarse especial atención a garantizar la financiación a largo plazo para todo el ciclo de vida de la estrategia nacional de ciberseguridad, comprendida las fases de elaboración, ejecución y perfeccionamiento. Para más detalles sobre la atribución de recursos para la ejecución, véase "Atribución de recursos humanos y financieros para la ejecución" (sección 3.4.3) y para la financiación a largo plazo, véase "Atribución de presupuesto y recursos específicos" (sección 5.1.5).

La Figura 2 muestra las posibles interacciones y la distribución de funciones entre las diferentes partes y los comités.

Más referencias disponibles en la página 55.

Figura 2 *– Partes interesadas*



3.2 Fase II: Inventario y análisis

El objetivo de esta fase es recopilar datos para evaluar el panorama nacional de la ciberseguridad y la situación presente y futura de los riesgos en el campo de la ciberseguridad con el fin de obtener información a los efectos de redactar y elaborar la estrategia nacional de ciberseguridad. El resultado de este ejercicio debe ser un informe destinado al Comité Directivo en el que se describa la postura estratégica nacional en materia de ciberseguridad y la situación en cuanto a los riesgos.

Antes de comenzar a redactar el texto de la estrategia, la autoridad responsable del proyecto debe analizar y evaluar meticulosamente la información recopilada durante la fase de inventario para asegurarse de que se han detectado las deficiencias en la capacidad de ciberseguridad y presentado opciones para subsanarlas. El análisis debe culminar en una evaluación de la medida en la que los entornos políticos, reglamentarios y operativos existentes cumplen los objetivos estipulados en la estrategia, indicando sus deficiencias.

Asimismo, debe utilizarse para identificar problemas concretos importantes, como carencias en materia de educación y formación.

Por último, el análisis debe culminar en una evaluación de todos los resultados pertinentes y deseados para la estrategia, así como de los posibles efectos y resultados de los medios escogidos.

Más referencias disponibles en la página 55.

3.2.1 Evaluación del panorama nacional de ciberseguridad

Para que la estrategia nacional de ciberseguridad sea eficaz, debe mostrar la postura del país en materia de ciberseguridad. A tal efecto, se debe realizar un análisis de los puntos fuertes y débiles de la ciberseguridad existente en el país y se debe consultar los materiales y documentos importantes en colaboración con las entidades pertinentes del gobierno, el sector privado y la sociedad civil. Esta etapa debe basarse en el principio de enfoque integral y prioridades adaptadas (descritas en la sección 4.2).

En el marco de estas actividades, la autoridad responsable del proyecto debe identificar los activos y servicios esenciales para el buen funcionamiento de la sociedad y la economía, y catalogar la normativa, los reglamentos, las políticas, los programas y las capacidades nacionales existentes en relación con la ciberseguridad. La autoridad responsable del proyecto también debe determinar los mecanismos de reglamentación no vinculante existentes, como las asociaciones entre los sectores público y privado, e inventariar las capacidades que se han desarrollado para hacer frente a los problemas de ciberseguridad, como los equipos nacionales de intervención en caso de emergencia informática (EIEI). Además, se deben determinar y asignar las funciones y responsabilidades de los

organismos públicos existentes con un mandato en materia de ciberseguridad, como los reguladores o los organismos de protección de datos.

Por otra parte, se deben recopilar datos conexos que contribuyan a conocer la postura de ciberseguridad del país, por ejemplo: información sobre los programas nacionales de ciberseguridad existentes, iniciativas internacionales, proyectos del sector privado, programas de TIC, de cibereducación y de desarrollo de capacidades, iniciativas de investigación y desarrollo en materia de ciberseguridad; datos sobre la penetración de Internet y las tasas de infección, adopción de las TIC, adelantos tecnológicos; y perspectivas sobre las futuras tendencias y amenazas de las TIC y la ciberseguridad.

También debe incluirse en este análisis la información pertinente proporcionada por el sector privado, las instituciones de investigación y otros grupos interesados. Para los países en desarrollo, también es fundamental registrar las iniciativas de colaboración con los asociados para el desarrollo a fin de coordinar la asistencia técnica y las inversiones.

Por último, la autoridad responsable del proyecto también debe analizar la información similar a escala regional e internacional y examinar las estrategias e iniciativas específicas de cada sector.

3.2.2 Evaluación del panorama de ciberriesgos

Partiendo de la información recopilada en la etapa anterior, la autoridad responsable del proyecto debe evaluar los riesgos que corre el país debido a la dependencia digital. Para ello puede recurrir a la identificación de los activos digitales nacionales, tanto públicos como privados, sus interdependencias, vulnerabilidades y amenazas, y a una estimación de la probabilidad y los posibles efectos en caso de incidente cibernético.

Esta actividad integra el principio de gestión de riesgos y resiliencia (sección 4.6), según el cual la gestión de riesgos es fundamental para aprovechar plenamente los beneficios del entorno digital en pro del desarrollo socioeconómico. Además, esta evaluación inicial de riesgos puede servir de base para futuras evaluaciones de riesgos más específicas (en la sección 5.2 figura más información sobre el principio de gestión de riesgos y resiliencia y sobre cómo llevar a cabo la evaluación de riesgos).

3.3 Fase III: Elaboración de la estrategia nacional de ciberseguridad

El objetivo de esta fase es elaborar el texto de la estrategia con la participación de los principales interesados del sector público, el sector privado y la sociedad civil a través de una serie de consultas públicas y grupos de trabajo. Este grupo más amplio de interesados, coordinado por la autoridad responsable del proyecto, se encargará de definir la visión general y el alcance de la estrategia, establecer

los objetivos de alto nivel, hacer un inventario de la situación actual (detallado en la fase II), priorizar los objetivos con arreglo a su incidencia en la sociedad, el ciudadano y la economía, y garantizar los recursos financieros necesarios. En esta fase se deben tomar en consideración todos los principios intersectoriales (sección 4) y las buenas prácticas (sección 5) que se detallan en esta guía.

3.3.1 Elaboración de la estrategia nacional de ciberseguridad

Una vez finalizada la fase de inventario y análisis, la autoridad responsable del proyecto, en colaboración con el Comité Directivo, debe comenzar a redactar la estrategia. Podrían crearse grupos de trabajo especializados para estudiar temas concretos o para redactar diferentes secciones de la estrategia. Los grupos de trabajo deben seguir los procesos establecidos en la fase de iniciación, ajustándolos según sea necesario.

La estrategia debe dar la orientación general de la ciberseguridad para el país; expresar una visión y un alcance claros; establecer los objetivos que deben alcanzarse dentro de plazos concretos; y priorizarlos en términos de su incidencia en la sociedad, la economía y la infraestructura. Además, debe identificar posibles formas de proceder, incentivar los esfuerzos de ejecución; y efectuar la atribución de los recursos necesarios para hacer posibles todas estas actividades. La estrategia también puede incluir algunos de los resultados obtenidos en la fase de inventario y análisis.

Al igual que en la etapa relativa a la planificación de la elaboración de la estrategia, el documento propiamente dicho debe proponer un marco de gobernanza claro (sección 5.1) que defina las funciones y responsabilidades de las principales partes. Esto incluye la identificación de la entidad responsable de la gestión y evaluación de la estrategia, así como de una entidad responsable de su gestión y ejecución en general, ya sea una autoridad central o un consejo nacional de ciberseguridad.

La estrategia también debe definir o confirmar el mandato de las diferentes entidades responsables de iniciar y preparar políticas y reglamentos de ciberseguridad en el país. Además, debe definir las responsabilidades y tareas de las entidades responsables de recopilar información sobre amenazas y vulnerabilidades, responder a los incidentes cibernéticos (por ejemplo, los EIEI nacionales), reforzar la preparación y gestionar las crisis. También debe velar por que se establezca sin ambages cómo interactúan todas estas entidades entre sí y con la autoridad central.

3.3.2 Consulta multipartita

Como se ha mencionado anteriormente, la participación de las diferentes partes es crucial para que la estrategia tenga éxito. A fin de garantizar que la estrategia final aúne una visión común, el borrador del documento debe divulgarse a un amplio grupo de interesados, no sólo a aquellos que participaron en el proceso de elaboración de la estrategia. Para ello se puede recurrir a varias vías, como consultas en línea, talleres de validación y grupos de trabajo adicionales. Cabe esperar que las opiniones y los comentarios recibidos tras este proceso se utilicen para finalizar la estrategia.

3.3.3 Aprobación oficial

En la etapa final del desarrollo de la estrategia, la autoridad responsable del proyecto debe asegurarse de que el Ejecutivo adopte oficialmente la estrategia. Este proceso de adopción oficial variará según el país y dependerá de la forma en que se defina la estrategia dentro del marco legislativo. Por ejemplo, podría adoptarse mediante un procedimiento parlamentario o un decreto gubernamental.

Además, es fundamental que la estrategia cuente con la aprobación de las más altas instancias del gobierno no sólo durante su preparación, sino que este compromiso continúe durante la fase de ejecución. Los funcionarios pertinentes deben rendir cuentas y contar con recursos y capital político.

3.3.4 Publicación de la estrategia

La estrategia debe ser un documento público y de fácil acceso. Su amplia disponibilidad garantizará que los ciudadanos conozcan las prioridades y los objetivos del gobierno en materia de ciberseguridad y también resultará útil en toda campaña destinada a aumentar la sensibilización sobre este particular. En caso de que la estrategia vaya acompañada de un Plan de Acción, éste debe indicar las oportunidades adicionales de participación y cooperación con la sociedad civil y el sector privado.

Más referencias disponibles en la página 55.

3.4 Fase IV: Ejecución

La fase de ejecución es la más importante de todo el ciclo de vida de la estrategia nacional de ciberseguridad. Para que la estrategia tenga éxito, es fundamental enfocar de manera estructurada su ejecución, con los recursos humanos y financieros adecuados, enfoque que debe considerarse parte de su desarrollo. La fase de ejecución suele basarse en un Plan de Acción, que orienta las diversas actividades previstas.

3.4.1 Elaboración del Plan de Acción

La ejecución de la estrategia, al igual que su elaboración, no puede ser responsabilidad exclusiva de una sola autoridad. Por el contrario, requiere la participación y coordinación de distintas partes del gobierno y el apoyo de la sociedad civil y del sector privado. El Plan de Acción, preparado de acuerdo con el principio de atribución clara de responsabilidades, funciones y recursos (sección 4.8), puede contribuir a la ejecución efectiva de la estrategia.

La elaboración del Plan de Acción es casi tan importante como el propio plan. El proceso, articulado por la autoridad responsable del proyecto, debe servir de mecanismo para reunir a las partes pertinentes con el fin de concertar objetivos y resultados, así como para coordinar esfuerzos y aunar recursos.

3.4.2 Determinación de las iniciativas que han de llevarse a cabo

La estrategia nacional de ciberseguridad describe los objetivos del gobierno y los resultados que desean alcanzar en las diferentes esferas prioritarias identificadas. En el Plan de Acción, la autoridad responsable del proyecto, en coordinación con las partes interesadas pertinentes, debe determinar las iniciativas específicas de cada esfera prioritaria que contribuirán a alcanzar esos objetivos. Como ejemplos se puede citar, entre otros, la organización de simulacros de ciberseguridad, el establecimiento de criterios de seguridad para infraestructuras esenciales o la instauración de un marco de notificación de incidentes.

El cronograma y los esfuerzos necesarios para la ejecución de estas iniciativas deben ser priorizados de acuerdo con su importancia para garantizar que los recursos escasos se aprovechen adecuadamente. A tal efecto, podrían tomarse en consideración los resultados y conclusiones de la fase II (Inventario y análisis), concretamente en lo que se refiere a la "Evaluación del panorama de ciberriesgos " (sección 3.2.2).

3.4.3 Asignación de recursos humanos y financieros para la ejecución

Una vez identificadas las iniciativas prioritarias, la autoridad responsable del proyecto debe designar a las entidades gubernamentales que se encargarán de cada una de esas iniciativas. A su vez, esas entidades gubernamentales serán responsables de la ejecución de cada una de las iniciativas concretas que se les asigne y deben coordinar sus esfuerzos con otros interesados pertinentes durante el proceso de ejecución.

Para garantizar que estas entidades puedan lograr los resultados esperados, la autoridad responsable del proyecto debe evaluar si se les ha otorgado un mandato adecuado -jurídico o de otra índole- para la ejecución. La autoridad responsable del proyecto también debe colaborar con los encargados de las iniciativas del caso para comprender qué recursos necesitan para llevar a buen término su labor. Esta evaluación debe incorporar los recursos humanos, la pericia y la financiación necesaria. La autoridad responsable del proyecto debe entonces colaborar con los encargados de las iniciativas para ayudarles a identificar y obtener los recursos necesarios con arreglo a las estructuras financieras administrativas del país.

3.4.4 Cronogramas y métricas

El último componente fundamental del Plan de Acción es la definición de métricas específicas e indicadores fundamentales de rendimiento para evaluar cada una de las iniciativas emprendidas, como por ejemplo si el país llevó a cabo una campaña de sensibilización sobre la importancia de compartir información, organizó y ejecutó un simulacro de ciberseguridad con el sector de infraestructuras esenciales, o aprobó una ley de seguridad básica. También deben establecerse plazos específicos para la ejecución.

Las métricas y los indicadores fundamentales de rendimiento deben ser desarrollados por la autoridad responsable del proyecto en colaboración con los respectivos encargados de las iniciativas. Se debe alentar a estos últimos a definir y mantener un conjunto pormenorizado de indicadores que faciliten la evaluación de la eficiencia y eficacia de las iniciativas durante su ejecución y una vez finalizadas.

Más referencias disponibles en la página 55.

3.5 Fase V: Supervisión y evaluación

En esta fase, la autoridad competente debería concebir un proceso oficial de supervisión y evaluación de la estrategia. En la fase de supervisión, el gobierno debe asegurarse de que la estrategia se aplica con arreglo a su Plan de Acción. En la fase de evaluación, el gobierno y su autoridad competente deben determinar si la estrategia sigue siendo pertinente en vista de la evolución de los riesgos, si sigue respondiendo a los objetivos del gobierno y qué ajustes son necesarios.

3.5.1 Establecimiento de un proceso oficial

Para garantizar una supervisión y una evaluación eficaces durante la ejecución de la estrategia, el gobierno tendrá que identificar una entidad independiente que se encargue de supervisar y evaluar el progreso y la eficiencia de la ejecución. Lo ideal sería que la entidad participara en la definición de métricas adecuadas de supervisión y evaluación para la ejecución de la estrategia, del correspondiente Plan de Acción y de las iniciativas conexas, que debe realizarse durante las fases de producción e iniciación.

La supervisión y medición del rendimiento y de la aplicación satisfactoria del plan de ejecución de la estrategia deben formar parte de los mecanismos de gobernanza que establezca el país. La evaluación continua del plan de ejecución (es decir, lo que marcha bien y lo que no) aporta información sobre la estrategia. Los mecanismos de buena gobernanza con respecto a la aplicación de la estrategia también deben deslindar claramente la rendición de cuentas y la responsabilidad de garantizar una ejecución satisfactoria. El establecimiento de métricas o indicadores fundamentales de rendimiento (IFR) para objetivos a corto, medio y largo plazo ayuda a reforzar los mecanismos de gobernanza y gestión. Los indicadores o métricas fundamentales de rendimiento deben ser:

- **Específicos**: destinados a mejorar un aspecto específico.
- **Cuantificables:** cuantificar o al menos ser indicativo del progreso.
- **Viables:** indicar qué resultados pueden lograrse de manera realista, dados los recursos disponibles.
- **Con responsabilidades:** especificar quiénes son los encargados
- **Con plazos:** especificar cuándo se lograrán los resultados.

El establecimiento de criterios permitirá supervisar mejor las medidas adoptadas y pondrá de relieve los aspectos susceptibles de mejora. Además, la asignación presupuestaria debe corresponderse con los niveles de ambición y complejidad del efecto deseado.

3.5.2 Supervisión de los progresos en la ejecución de la estrategia

La entidad responsable de supervisar los progresos en la ejecución de la estrategia debe actuar de conformidad con el calendario convenido a lo largo de todo el ciclo de vida de la estrategia. El resultado de esa actividad de supervisión (por ejemplo, un informe) debe consignar todas las diferencias respecto de los plazos acordados y las razones de dichos retrasos, como el cambio de prioridades, la insuficiencia de personal o de recursos, etc. Esta información es adicional a la información periódica que los encargados de los diferentes aspectos de la ejecución de la estrategia deben comunicar a la autoridad responsable del proyecto.

Este método garantizará que las partes pertinentes rindan cuentas del cumplimiento de los compromisos contraídos; también garantizará que se identifiquen con prontitud todos los problemas que surjan durante la ejecución. A su vez, el gobierno podrá rectificar la situación o adaptar sus planes en consecuencia basándose en las lecciones extraídas durante la ejecución.

3.5.3 Evaluación de los resultados de la estrategia

Además de evaluar los progresos mediante las métricas acordadas, es importante también evaluar periódicamente los resultados y compararlos con los objetivos establecidos. Esta evaluación es fundamental para comprender si los objetivos de la estrategia se están cumpliendo o si deben tomarse diferentes acciones. En este proceso, también es necesario reexaminar periódicamente el contexto de riesgos en general para comprender si se han producido cambios externos que puedan afectar a los resultados de la estrategia. En la práctica, este proceso sirve de pequeña revisión del perfil de evaluación de los riesgos para el país.

La evaluación, junto con las recomendaciones asociadas, debe recopilarse en un informe destinado a la autoridad responsable del proyecto, en el cual debe proponerse alternativas para actualizar el Plan de Acción y garantizar que éste sigue siendo vigente y adecuado para los cambios que se producen en la política y en el panorama de riesgos.

En última instancia, los informes elaborados a lo largo del ciclo de vida de la estrategia también deben servir de base para el examen general de la estrategia nacional de ciberseguridad, de conformidad con el calendario establecido en la fase inicial. Esta revisión global no sólo debe tomar en consideración los progresos logrados y los cambios en el entorno externo, sino también replantear las propias prioridades y objetivos del gobierno.

Más referencias disponibles en la página 55.

4 Principios generales

En esta sección se presentan nueve principios intersectoriales que, tomados en su conjunto, pueden contribuir a la elaboración de una estrategia nacional de ciberseguridad global y prospectiva.

Estos principios son aplicables a todas las esferas prioritarias indicadas en el presente documento. Deben tenerse en cuenta en todas las etapas del proceso de elaboración de la estrategia nacional, desde la redacción del documento de la estrategia nacional hasta su ejecución.

El orden de los principios que se indican a continuación responde a una lógica narrativa más que un orden de importancia.

4.1 Visión

La estrategia debe establecer una visión clara de todo el gobierno y de toda la sociedad.

La estrategia tiene más probabilidades de tener éxito cuando establece una visión que ayuda a todas las partes interesadas a comprender lo que está en juego, por qué se necesita la estrategia (contexto), cuáles son sus fines (objetivos), así como de qué se trata y a quién afecta (alcance).

Cuanto más clara sea la visión, más fácil será para los dirigentes y las principales partes garantizar un enfoque más integral, coherente y congruente. Una visión clara también facilita la coordinación, la cooperación y la ejecución de la estrategia entre las partes interesadas pertinentes. Debe formularse a un nivel suficientemente alto y tener en cuenta la naturaleza dinámica del entorno digital.

Los objetivos y el calendario de aplicación de la estrategia deberían ajustarse a esta visión.

Más referencias disponibles en la página 56.

4.2 Enfoque integral y prioridades adaptadas

La estrategia debe ser el resultado de un entendimiento y un análisis globales del entorno digital en su conjunto, pero adaptada a las circunstancias y prioridades del país.

La ciberseguridad no es meramente una dificultad técnica, sino una cuestión compleja y polifacética, cuyos aspectos trascienden la prosperidad socioeconómica hasta ámbitos tales como la observancia de la ley, la seguridad nacional e internacional, las relaciones internacionales, las negociaciones comerciales, el desarrollo sostenible, etc.

Es importante comprender todos los aspectos de la ciberseguridad y cómo se interrelacionan, se complementan o compiten entre sí. Una vez comprendidos estos aspectos y tras realizar un análisis del contexto específico del país, pondrán definirse las prioridades con arreglo a los objetivos y los plazos de ejecución de la estrategia. Las prioridades permitirán establecer objetivos y plazos concretos, así como asignar los recursos necesarios.

Las prioridades que se consignen en la estrategia nacional de ciberseguridad variarán según el país. Algunos de los temas relativos a la ciberseguridad pueden abordarse en el mismo documento estratégico o en documentos separados (por ejemplo, los aspectos digitales de la seguridad y la defensa nacional pueden integrarse en una estrategia nacional de seguridad o defensa).

Más referencias disponibles en la página 56.

4.3 Inclusividad

La estrategia debe elaborarse con la participación activa de todas las partes interesadas pertinentes y debe definir sus necesidades y responsabilidades.

El entorno digital se ha convertido en un aspecto fundamental para el gobierno, las empresas y los ciudadanos. Estos grupos tienen que afrontar riesgos para la ciberseguridad y comparten un nivel de responsabilidad en su gestión, que depende de su función. Si bien ésta puede ser una tarea difícil, la identificación e implicación de todas las partes interesadas es fundamental para el buen desarrollo y ejecución de la estrategia nacional de ciberseguridad. Este planteamiento ayudará a comprender las necesidades de las partes interesadas y su conocimiento y experiencia únicos, facilitando así la cooperación para lograr los objetivos de la estrategia.

Para fomentar la inclusividad, la estrategia debe ser un documento público.

Más referencias disponibles en las páginas 56 y 57.

4.4 Prosperidad económica y social

La estrategia debe fomentar la prosperidad socioeconómica y maximizar la contribución de las TIC al desarrollo sostenible y la inclusión social.

El entorno digital puede acelerar el crecimiento económico y el progreso social, promover valores sociales fundamentales, mejorar la prestación y la capacidad de los servicios públicos, facilitar el comercio internacional y promover la buena gobernanza.

La creciente dependencia del entorno digital para el funcionamiento de las sociedades hace necesario prestar mayor atención a la ciberseguridad. Sin embargo, la ciberseguridad no es una meta en sí misma; la estrategia debe estar en consonancia con los objetivos socioeconómicos más generales del país y generar la confianza y fe necesarias para ayudar a alcanzar estos objetivos y para proteger al país contra las ciberamenazas.

Más referencias disponibles en la página 57.

4.5 Derechos humanos fundamentales

La estrategia debe respetar los valores fundamentales y ser coherentes con los mismos.

Debe reconocer el hecho de que los mismos derechos que tiene el ciudadano fuera de línea también deben protegerse en línea. Debe respetar los derechos fundamentales universalmente acordados, comprendidos, entre otros, los consignados en la Declaración Universal de Derechos Humanos de las Naciones Unidas y en el Pacto Internacional de Derechos Civiles y Políticos, así como en los marcos jurídicos multilaterales o regionales pertinentes.

Debe prestar atención a la libertad de expresión, la privacidad de las comunicaciones y la protección de los datos personales. En particular, la estrategia debe evitar que se lleve a cabo vigilancia, interceptación de comunicaciones o análisis de datos personales de manera arbitraria, injustificada o ilícita.

Al equilibrar las necesidades del Estado con las del ciudadano, la estrategia debe velar por que, la eventual vigilancia, interceptación de las comunicaciones o recopilación de datos se efectúen exclusivamente en el contexto de una investigación o causa judicial específica, autorizado por la autoridad nacional competente y sobre la base de un marco jurídico público, preciso, exhaustivo y no discriminatorio que permita una supervisión eficaz y garantías y recursos procesales.

Más referencias disponibles en las páginas 57 y 58.

4.6 Gestión de riesgos y resiliencia

La estrategia debe permitir una gestión eficaz de los riesgos para la ciberseguridad y mejorar la resiliencia de las actividades socioeconómicas.

Si bien el entorno digital ofrece a las partes interesadas oportunidades económicas y sociales, también las expone a diversos riesgos de ciberseguridad. Por ejemplo, cuando las organizaciones utilizan las TIC para fomentar la innovación, aumentar la productividad y mejorar la competitividad, o cuando los gobiernos despliegan

sus servicios en línea, pueden producirse incidentes de ciberseguridad que se traduzcan en pérdidas económicas, daños a la reputación, interrupción de las operaciones, menoscabo de la innovación, etc. Al igual que con otros tipos de riesgo, el riesgo para la ciberseguridad no puede eliminarse por completo, pero puede gestionarse y minimizarse.

Para superar estas dificultades, la estrategia debe instar a las entidades a dar prioridad a sus inversiones en ciberseguridad y a gestionar los riesgos de forma proactiva. Dependiendo del nivel de riesgo que la entidad desee asumir, se debe mantener un equilibrio entre las medidas de seguridad y los beneficios potenciales, teniendo en cuenta la naturaleza dinámica del entorno digital. La estrategia también debe reconocer la necesidad de gestionar continuamente los riesgos y facilitar un planteamiento coherente entre entidades interdependientes.

La atención que se preste a la gestión de riesgos contribuirá también a que las partes estén preparadas para posibles incidentes de seguridad, garantizando la resiliencia de la actividad socioeconómica en el país. En ese sentido, la estrategia debe alentar la adopción de medidas de continuidad operativa, que incluyan la gestión de incidentes y de crisis, así como planes de recuperación.

Más referencias disponibles en la página 58.

4.7 Conjunto adecuado de instrumentos políticos

La estrategia debe utilizar los instrumentos políticos más adecuados disponibles para alcanzar cada uno de sus objetivos, teniendo en cuenta las circunstancias específicas del país.

Los objetivos en materia de ciberseguridad del gobierno sólo se alcanzarán si se produce un cambio de comportamiento entre todas las partes involucradas. En la mayoría de los casos, los gobiernos tienen a su disposición diferentes mecanismos e instrumentos de política para lograr ese resultado. Cabe citar, por ejemplo, la legislación, la reglamentación, la normalización, los programas y mecanismos de incentivos y de intercambio de información, los programas de educación, el intercambio de las prácticas idóneas, el establecimiento de pautas de comportamiento esperadas y la creación de comunidades de confianza. Cada uno de estos instrumentos presenta ventajas e inconvenientes, tiene costos diferentes y produce resultados distintos.

Los mejores resultados pueden lograrse seleccionando el instrumento político más apropiado para cada objetivo concreto y llegando a un equilibrio en la utilización de las diferentes herramientas.

Más referencias disponibles en la página 59.

4.8 Dirigentes, funciones y atribución de recursos claramente estipulados

La estrategia debe definirse en las más altas instancias del gobierno, que por tanto serán responsables de asignar las funciones y responsabilidades pertinentes y de atribuir suficientes recursos humanos y financieros.

La ciberseguridad debe promoverse y mantenerse en las más altas esferas del gobierno. Además, para garantizar la rendición de cuentas y el progreso, es necesario identificar los coordinadores de las distintas esferas de actividad, y todas las partes implicadas deben entender claramente sus respectivas funciones y responsabilidades.

La estrategia también debe asignar los recursos humanos, financieros y materiales necesarios para su ejecución. Este principio debe aplicarse tanto al proceso de elaboración de la estrategia como a la preparación de su Plan de Acción.

Más referencias disponibles en la página 59.

4.9 Entorno de confianza

La estrategia debe contribuir a crear un entorno digital en el que los ciudadanos y las empresas puedan confiar.

El fomento de la confianza en el ecosistema digital nacional, en el que se protegen los derechos e intereses de los usuarios y se garantiza la seguridad de los datos y de los sistemas, es esencial para poder aprovechar plenamente el potencial de las oportunidades sociales, políticas y económicas que ofrecen las tecnologías de la información y la comunicación. La estrategia debe permitir la adopción de políticas, procesos y medidas a escala nacional que aporten seguridad a los servicios esenciales que se prestan al ciudadano (como el gobierno electrónico, el comercio electrónico y las transacciones financieras digitales, entre otros) basados en las tecnologías de la información y la comunicación. Este tipo de acciones instaurará el principio de confianza no sólo entre la población en general, sino también dentro de las organizaciones públicas y privadas que ofrezcan sus servicios basados en las TIC a los ciudadanos.

Más referencias disponibles en la página 59.

5 Buenas prácticas en la estrategia nacional de ciberseguridad

La ciberseguridad afecta a numerosos aspectos del desarrollo socioeconómico y se ve afectada por diversos factores dentro del contexto nacional.

Por ese motivo, esta sección presenta un conjunto de buenas prácticas que pueden mejorar la integridad y eficacia de la estrategia y que, a su vez, permiten adaptarla al contexto nacional.

Estas buenas prácticas se agrupan en distintas esferas de interés, que se corresponden con los temas generales de una estrategia nacional de ciberseguridad. Si bien tanto las esferas de interés como los aspectos se han presentado aquí como ejemplos de buenas prácticas, es particularmente importante que estas últimas se consideren en el contexto nacional, ya que algunas pueden no ser pertinentes para la situación específica de un país. Los países deben determinar y aplicar las buenas prácticas que sirvan para alcanzar sus propios objetivos y prioridades de acuerdo con la visión definida en su estrategia (sección 4). El orden de las prácticas o esferas de interés que figuran a continuación no debe considerarse indicativo del nivel de importancia o prioridad.

5.1 Esfera prioritaria 1 – Gobernanza

En esta esfera prioritaria se introducen aspectos de buenas prácticas cuya inclusión en el texto de la estrategia debe sopesarse al examinar la estructura de gobernanza de la ciberseguridad nacional. La estrategia debe definir claramente los objetivos y las ambiciones que el gobierno tiene en mente en materia de ciberseguridad, así como describir las funciones y responsabilidades necesarias para garantizar su ejecución.

A tal efecto, la estrategia debe identificar y facultar a la autoridad competente que se encargará de su ejecución; establecer un mecanismo para identificar e incluir a las entidades gubernamentales afectadas o responsables de la ejecución de la estrategia; incluir objetivos específicos, cuantificables, viables, basados en resultados y con plazos concretos en el plan de ejecución de la estrategia; y reconocer la necesidad de destinar recursos (por ejemplo, voluntad política, financiación, tiempo y personal) para lograr los resultados deseados.

5.1.1 Garantizar el apoyo de las altas instancias

La estrategia debe contar con el respaldo oficial de las altas instancias gobierno. Este respaldo sirve para dos propósitos importantes. En primer lugar, aumenta la probabilidad de que se asignen recursos suficientes y de que los esfuerzos de coordinación tengan éxito. En segundo lugar, envía una señal al ecosistema nacional en general de la importancia que el país confiere a la ciberseguridad.

5.1.2 Establecer una autoridad competente en materia de ciberseguridad

La estrategia debe identificar una autoridad nacional competente en materia de ciberseguridad, es decir, un dirigente (individuo o entidad) que ocupe un cargo elevado y profundamente arraigado en las altas instancias del gobierno para dar orientaciones, coordinar la acción y supervisar la ejecución de la estrategia.

Dicha autoridad nacional competente en materia de ciberseguridad debe actuar también como entidad gestora para definir y aclarar las funciones, responsabilidades, procesos, potestades de decisión y tareas necesarias para garantizar la ejecución efectiva de la estrategia. Esto incluye la identificación de los agentes que supervisarán la ejecución de la estrategia y el establecimiento de objetivos de rendimiento para diversos departamentos ministeriales o gubernamentales, instituciones o personas responsables de aspectos específicos de la estrategia y el Plan de Acción conexo. Este enfoque puede requerir estructuras políticas o jurídicas adicionales que los faculten para llevar a cabo sus misiones.

Dado que la ciberseguridad abarca muy distintas esferas, es importante garantizar que la autoridad nacional competente tenga la capacidad de implicar y dirigir a las partes pertinentes.

5.1.3 Garantizar la cooperación intragubernamental

La estrategia debe establecer un mecanismo para identificar e incluir a las entidades gubernamentales afectadas o responsables de su ejecución. El compromiso, la coordinación y la cooperación intragubernamentales son funciones básicas de esas instituciones gubernamentales y son además necesarias para velar por que los mecanismos de gobernanza (es decir, las normas) y los recursos produzcan los resultados previstos en la estrategia.

La comunicación y la coordinación eficaces garantizan que todos los ministerios y organismos gubernamentales conozcan las respectivas autoridades, misiones y tareas de cada uno. Sin embargo, el compromiso consiste en apoyar políticas coherentes a lo largo del tiempo para garantizar que se cumplan las promesas dimanantes de la estrategia. Como ejemplo de mecanismo de coordinación cabe citar la celebración de reuniones periódicas en las que participen todas las partes pertinentes en los planes de acción que se examinarán conjuntamente. Un ejemplo de mecanismo de cooperación sería la creación de un grupo de trabajo intragubernamental para abordar una cuestión concreta. Un ejemplo de compromiso es la coherencia entre la agenda de política interior y la de política exterior del país, de modo que un ministerio no socave la credibilidad de otro al representar posiciones diferentes en el mismo ámbito político.

5.1.4 Garantizar la cooperación intersectorial

La estrategia debe mostrar un entendimiento común de las dependencias que el gobierno tiene con respecto al sector privado y otras partes nacionales (y viceversa) a los efectos de garantizar la ciberseguridad. A tal efecto, debe articular cómo el gobierno logrará que se impliquen estas partes y definirá sus funciones y responsabilidades. Por ejemplo, la estrategia debe identificar una red nacional de

puntos de contacto autorizados de las industrias esenciales para el funcionamiento y la recuperación de servicios e infraestructuras fundamentales.

5.1.5 Asignar presupuesto y recursos específicos

La estrategia debe especificar la asignación de recursos específicos y adecuados para su ejecución, mantenimiento y revisión. Para lograr una postura nacional eficaz en materia de ciberseguridad se requiere una financiación suficiente, coherente y continua. Los recursos deben definirse en términos económicos (es decir, presupuesto dedicado), personal, material, así como las relaciones y asociaciones, el compromiso político continuo y el liderazgo necesarios para su buena ejecución. La dotación de recursos para los objetivos y tareas de la estrategia no debe considerarse una iniciativa aislada. Los recursos pueden ser asignados por tarea u objetivo, o por entidad gubernamental.

El gobierno también podría considerar la posibilidad de establecer un presupuesto central destinado a ciberseguridad, gestionado por un mecanismo centralizado para la gobernanza de la ciberseguridad. Ya se trate de reunir fuentes de financiación diversas en un programa coherente e integrado o de crear un presupuesto intragubernamental unificado, el programa general se debe gestionar y aplicar por etapas para garantizar una ejecución satisfactoria de la estrategia.

5.1.6 Elaborar un plan de ejecución

La estrategia debe ir acompañada de un plan de ejecución, o remitir a uno, en el que se describa con mayor detalle la forma en que se lograrán sus objetivos estratégicos. Para que el plan de ejecución resulte efectivo debe identificar la entidad responsable de cada tarea y objetivo, los recursos necesarios para ejecutarlos a lo largo del tiempo (corto, mediano y largo plazo), los procesos que se utilizarán y los resultados esperados (sección 3.4 sobre Iniciación de la ejecución).

Más referencias disponibles en las páginas 60 y 61.

5.2 Esfera prioritaria 2 – Gestión de riesgos para la ciberseguridad nacional

En esta esfera prioritaria se introducen buenas prácticas para abordar la ciberseguridad mediante la gestión de riesgos. Como se estipula en el principio de gestión de riesgos y resiliencia (sección 4.2), se debe adoptar un enfoque de gestión de riesgos, ya que los ciberriesgos no se pueden eliminar por completo. Ahora bien, si el país tiene un buen conocimiento de los riesgos a los que está expuesto, podrá gestionarlos más eficazmente. Por lo que se refiere a la evaluación de los riesgos, el enfoque debe concentrarse en identificar las interdependencias y, además, examinar los riesgos derivados de las dependencias transfronterizas. El mecanismo de gestión de riesgos debe tomar en consideración todo el ciclo de vida, desde el desarrollo o adquisición hasta la operación y la sustitución.

También es importante señalar que, como las amenazas a la ciberseguridad son extremadamente dinámicas e impredecibles, cualquier enfoque de gestión de riesgos debe revisarse periódicamente. Asimismo, la estrategia debe planificar el

seguimiento y la evaluación de las actividades de gestión de riesgos para garantizar mejoras continuas.

5.2.1 Definir un mecanismo de gestión de riesgos

La estrategia debe definir un mecanismo coherente para la gestión de riesgos que deben aplicar todas las entidades gubernamentales y los operadores de infraestructura esencial identificados en el plano nacional. El mecanismo debe permitir la identificación de los activos y servicios esenciales para el buen funcionamiento de la sociedad y la economía, así como las amenazas y los riesgos inherentes a los mismos.

El objetivo es desarrollar un registro nacional de riesgos, almacenado y comunicado de forma segura, que permita al gobierno supervisar los riesgos y las soluciones adoptadas con el fin de gestionarlos. Además, el mecanismo debe contar con un método de establecimiento de prioridades basado en el cálculo de la probabilidad de que se materialicen los riesgos y sus repercusiones. Además, debe especificar las responsabilidades de las entidades fundamentes de cada sector en lo que respecta a la evaluación, aceptación y tratamiento de los riesgos para la ciberseguridad a escala nacional.

5.2.2 Identificar una metodología común para gestionar los riesgos para la ciberseguridad

La estrategia debe definir una metodología común para gestionar los riesgos para la ciberseguridad. Esto garantizará la eficiencia y la coherencia en todas las organizaciones y facilitará el intercambio de información sobre riesgos entre sistemas interdependientes. Debe favorecer una metodología basada en normas internacionales, ya que ello reduce los costos y mejora la interacción con el sector privado.

La metodología debe dar orientaciones sobre la asignación de funciones y responsabilidades para diversos aspectos de la gestión de riesgos, como la evaluación de las amenazas, la valoración de los activos, la ejecución y el mantenimiento de medidas de mitigación y la aceptación de riesgos residuales. La metodología debe incluir un programa de certificación para ayudar a evaluar y luego mejorar el cumplimiento.

Es importante señalar que, para la adquisición y el desarrollo de infraestructuras o servicios, la metodología de gestión de riesgos debe dar además orientaciones sobre cómo minimizar el riesgo mediante una arquitectura y un diseño seguros, reconociendo que se obtiene mayor seguridad cuando ésta es parte integrante del proceso de diseño de un producto, proceso o servicio (seguridad desde la fase de diseño).

5.2.3 Elaborar perfiles de riesgos sectoriales en materia de ciberseguridad

La estrategia debe exigir la utilización de perfiles de riesgos sectoriales en materia de ciberseguridad. Por perfil de riesgos sectorial se entiende un análisis cuantitativo de los tipos de amenazas a las que se enfrenta el sector. El objetivo del perfil de riesgos

es comprender los riesgos de una manera menos subjetiva mediante la asignación de valores numéricos a variables relacionadas con diferentes tipos de amenazas y el peligro que representan. La estrategia debería recomendar la elaboración de perfiles de riesgos para los sectores que el país considera fundamentales para su sociedad y su economía.

La utilización de perfiles de riesgos sectoriales sienta las bases para efectuar evaluaciones de riesgos más específicas de distintas organizaciones, aumenta la coherencia dentro y a través de todos los sectores a escala nacional y reduce los recursos necesarios para evaluar los riesgos que corren las organizaciones. Los perfiles deben actualizarse periódicamente para garantizar que se mantengan actualizados.

5.2.4 Establecimiento de políticas de ciberseguridad

La estrategia debe fomentar el establecimiento de políticas de ciberseguridad para entidades nacionales fundamentales, como por ejemplo las autoridades gubernamentales y los operadores de infraestructura esencial. Tales políticas, adoptadas de conformidad con el principio de conjunto adecuado de instrumentos políticos (sección 4.7), abarcarán los requisitos de gobernanza, operacionales y técnicos, definirán las funciones y responsabilidades de las partes interesadas y darán orientaciones o establecerán mecanismos específicos para estos temas.

Estas políticas podrían consistir en, por ejemplo, tener en cuenta la ciberseguridad en las etapas de adquisición o desarrollo, definir programas de intercambio de información, coordinar la divulgación de vulnerabilidades, establecer pautas mínimas de atención, especificar criterios de seguridad, definir programas de certificación para la observancia y exigir la notificación de incidentes cibernéticos.

La adopción de un planteamiento coordinado a escala nacional permitiría realizar una gestión más eficiente y eficaz de la ciberseguridad, armonizaría las prácticas y facilitar la coordinación y la interoperabilidad.

Más referencias disponibles en la página 61.

5.3 Esfera prioritaria 3 – Preparación y resiliencia

En esta esfera prioritaria se describe el panorama general de las buenas prácticas para el establecimiento y la sostenibilidad de capacidades nacionales eficaces destinadas a prevenir, detectar, mitigar y responder a los principales incidentes de ciberseguridad, así como a mejorar la capacidad general de resiliencia cibernética del país.

5.3.1 Establecer capacidades de respuesta a incidentes cibernéticos

La estrategia debe exigir el establecimiento de las capacidades nacionales adecuadas de intervención en caso de incidente para hacer frente a los problemas operativos de ciberseguridad. A menudo, esta capacidad se refiere al establecimiento de equipos de intervención en caso de emergencia informática (EIEI), equipos de intervención en caso de incidentes de seguridad informática (EIISI) o equipos de intervención en caso de incidente informático (EIII) con responsabilidad nacional.

Aunque la forma organizativa específica de los EIEI/EIISI/EIII puede variar (por ejemplo, nacional, gubernamental, sectorial, etc.) y no todos los países tienen las mismas necesidades y recursos, estos equipos especializados y dedicados deben desempeñar un conjunto de funciones tanto proactivas como reactivas, y prestar servicios preventivos y educativos. De este modo, estas entidades pueden aumentar la capacidad del país para reaccionar rápidamente ante ciberataques y recuperarse de sus consecuencias, así como mejorar su resistencia a las ciberamenazas, reduciendo las eventuales repercusiones económicas y operativas globales de los ciberataques de importancia nacional.

La estrategia también debe identificar y desarrollar mecanismos de cooperación y procedimientos de comunicación entre los equipos nacionales y sectoriales de respuesta a incidentes (de existir en el país), así como con las contrapartes internacionales.

5.3.2 Establecer planes de contingencia para gestionar crisis de ciberseguridad

La estrategia debe exigir la elaboración de un plan nacional de contingencia para situaciones de emergencia y de crisis en materia de ciberseguridad. El plan debe formar parte del plan nacional general de contingencia o estar en consonancia con él. También debe considerarse la posibilidad de crear un plan específico para la infraestructura esencial de información.

Este plan nacional de contingencia en materia de ciberseguridad debe tener en cuenta las conclusiones de las evaluaciones nacionales de riesgos y toda dependencia intersectorial que pudiera afectar a la continuidad de las operaciones de la infraestructura esencial, así como cualquier mecanismo de recuperación en caso de catástrofe. Además, debe proporcionar una perspectiva general de los mecanismos nacionales de respuesta a incidentes y clasificar los incidentes de ciberseguridad en función de su incidencia en los activos y servicios fundamentales.

5.3.3 Promover el intercambio de información

La estrategia debe exigir el establecimiento de mecanismos de intercambio de información que permitan compartir inteligencia e información útil sobre amenazas entre los sectores público y privado.

Los programas oficiales y oficiosos de intercambio de información pueden ayudar a fomentar la coordinación eficaz y las comunicaciones coherentes, precisas y adecuadas durante las actividades de restablecimiento y respuesta a incidentes; facilitar el intercambio rápido de inteligencia e información sobre amenazas entre las partes afectadas y otras partes interesadas; ayudar a comprender mejorar cómo y qué sectores se han visto afectados; difundir información sobre los métodos que pueden utilizarse para defender y mitigar los daños en los activos afectados; y, en última instancia, reducir las vulnerabilidades y la exposición junto con los riesgos que conllevan.

La estrategia debe identificar una o varias estructuras institucionales (es decir, autoridades competentes) responsables de transmitir información precisa y práctica entre la comunidad nacional de ciberseguridad, incluidos los sectores público y privado.

El intercambio de información debe ser un proceso bidireccional. Si los gobiernos están dispuestos a compartir la información que poseen, demostrarán así a las entidades del sector privado que el gobierno es realmente un asociado en el intercambio de información sobre amenazas y contribuirán a que los equipos de respuesta se concentren en las amenazas esenciales y estén mejor preparados para responder a ellas.

5.3.4 Realizar simulacros de ciberseguridad

La estrategia debe fomentar la organización y coordinación de simulacros de ciberseguridad y respuesta a incidentes a escala nacional e internacional. Estos pueden seguir diferentes formatos (por ejemplo, simulaciones o ejercicios en tiempo real) y dirigirse a las audiencias técnicas y a los poderes públicos.

Los simulacros de ciberseguridad y otros mecanismos de planificación de crisis pueden ayudar a los países a desarrollar la capacidad institucional necesaria para dar una respuesta eficaz a los incidentes, poner a prueba los procedimientos de gestión de crisis y los mecanismos de comunicación, verificar la capacidad operativa de los EIEI/EIISI/EIII para actuar bajo presión y ayudar a comprender cualquier dependencia intersectorial.

Análogamente, los simulacros internacionales de ciberseguridad pueden ayudar a fortalecer la capacidad de respuesta a los incidentes cibernéticos entre los Estados, comprender las dependencias transfronterizas, fomentar la confianza entre los países y mejorar los niveles generales de preparación y resiliencia internacional.

Más referencias disponibles en las páginas 62 y 63.

5.4 Esfera prioritaria 4 – Servicios de infraestructura esencial y servicios fundamentales

Esta esfera prioritaria trata de las buenas prácticas relacionadas con la protección de la infraestructura esencial (IE) y, en particular, la infraestructura esencial de la información (IEI). Si bien no existen definiciones universalmente reconocidas de estos dos términos y los gobiernos deben considerar qué entidades y servicios incluir en estas categorías en función de su propia evaluación nacional de riesgos, a los efectos de la presente guía estos términos se definen de la siguiente manera:

infraestructura esencial: término utilizado para designar los activos que son esenciales para el funcionamiento y la seguridad de la sociedad y la economía en un determinado país; y

infraestructura esencial de la información: sistemas de TI y TIC que desempeñan funciones esenciales de la infraestructura esencial del país.

Por otra parte, se puede aplicar el concepto de servicios fundamentales, refiriéndose a los servicios que resultan fundamentales para las actividades socioeconómicas indispensables.

En cualquier caso, como ejemplos de estos servicios cabe citar: energía (electricidad, petróleo y gas), transporte (aéreo, ferroviario, marítimo y por carretera), finanzas y banca (instituciones crediticias, centros de comercio y contrapartes centrales), asistencia sanitaria (organizaciones sanitarias, incluidos hospitales y clínicas privadas),

suministro y distribución de agua potable, servicios digitales y de telecomunicaciones (servicios de telefonía fija y móvil y suministro de infraestructura de Internet, como centrales Internet (IXP) y servicios de nombres de dominio, entre otros).

5.4.1 Establecer un planteamiento de gestión de riesgos para proteger los servicios e infraestructuras esenciales

La estrategia debería abordar la protección de infraestructura esencial y la infraestructura esencial (IE+IEI) de la información desde la perspectiva de la gestión de riesgos, de conformidad con el principio de gestión de riesgos y resiliencia (sección 4.6). A partir de la evaluación detallada de los riesgos se debe identificar la IE+IEI nacionales y los servicios fundamentales, cuya interrupción puede tener un impacto grave en la salud, la seguridad, la protección o el bienestar económico de los ciudadanos, o en el funcionamiento efectivo del gobierno o de la economía.

Además, también debe adoptarse un planteamiento basado en los riesgos para identificar y priorizar la ejecución de programas y políticas concebidas para proteger a la IE+IEI. A fin de facilitar la colaboración con el sector privado, también podría considerarse la posibilidad de adoptar un planteamiento de gestión de riesgos basado en normas internacionales.

5.4.2 Adoptar un modelo de gobernanza con responsabilidades bien definidas

La estrategia debe describir la estructura general de gobernanza, las funciones y las responsabilidades de las distintas partes interesadas en la protección de la IE+IEI. Como se estipula en el principio de definir claramente los dirigentes, las funciones y la atribución de recursos (sección 4.8), el programa eficaz y eficiente de protección de la infraestructura esencial requiere que las funciones y responsabilidades de las partes interesadas estén claramente definidas y que se establezca un mecanismo de coordinación para gestionar los problemas pendientes.

La IE+IEI no suelen ser propiedad del gobierno ni están controladas por éste, y los esfuerzos de protección de la IE+IEI por lo general trascienden las capacidades y el mandato de una sola entidad gubernamental. Por consiguiente, la designación de un coordinador general para la (ciber) seguridad de la IE+IEI, como un comité interinstitucional, puede ser de gran ayuda en los esfuerzos por proteger la infraestructura esencial.

El modelo de gobernanza para la protección de la IE+IEI debe incluir la identificación de las entidades gubernamentales a cargo de sectores específicos, las responsabilidades y la rendición de cuentas de los operadores de IE+IEI, así como los canales de comunicación y los mecanismos de cooperación entre los organismos públicos y privados para garantizar el funcionamiento y la recuperación de servicios e infraestructuras esenciales.

5.4.3 Definir criterios mínimos de ciberseguridad

La estrategia debe poner de relieve los marcos legislativos y reglamentarios existentes o proponer el desarrollo de nuevos marcos legislativos y reglamentarios que establezcan criterios mínimos de ciberseguridad que sirvan de referencia para, entre otros, los operadores de IE+IEI. Al definir estos criterios, deben tenerse en cuenta las

normas y prácticas idóneas reconocidas internacionalmente para garantizar mayor seguridad y eficiencia.

Los criterios mínimos de seguridad deben centrarse en los resultados, articulando lo que las organizaciones deben tratar de conseguir (por ejemplo, "controlar el acceso lógico a los recursos esenciales"), y no en cómo las organizaciones deben aplicar la seguridad (por ejemplo, "utilizar la autentificación de dos factores"), lo que a su vez permitirá al gobierno y a la industria beneficiarse de las mejoras continuas de la seguridad. Además, el método basado en los resultados para el desarrollo de estos criterios deja margen para la aplicación sectorial o las guías "prácticas", otorgando a las empresas la flexibilidad de actualizar periódicamente sus propias pautas para adaptarse a los cambios tecnológicos y los peligros del momento.

5.4.4 Utilizar muy diversos mecanismos del mercado

La estrategia debe tener en cuenta una gran diversidad de políticas para garantizar que todas las organizaciones e individuos se vean realmente incentivados a cumplir con sus responsabilidades en materia de ciberseguridad, en consonancia con los riesgos a los que se enfrentan y de conformidad con el principio de enfoque integral y prioridades adaptadas (sección 4.2).

Identificar las divergencias entre lo que los mercados pueden y deben realizar y lo que el entorno de riesgo requiere es un paso crucial para determinar cuándo y cómo aprovechar la gama de incentivos y factores disuasorios disponibles para mejorar la seguridad. A los efectos de fomentar la adopción de normas y prácticas de ciberseguridad en la IE+IEI, la estrategia debe indicar que el gobierno estudiará una serie de opciones políticas y mecanismos del mercado a su disposición.

5.4.5 Establecer asociaciones público-privadas

La estrategia debe fomentar la creación de asociaciones oficiales entre el sector público y el privado para aumentar la seguridad de la IE+IEI. Las asociaciones público-privadas son la piedra angular de la protección eficaz de la infraestructura esencial y de la gestión de los riesgos para la seguridad, tanto a corto como a largo plazo. Son esenciales para aumentar la confianza entre la industria y el gobierno.

Sin embargo, el establecimiento de asociaciones sostenibles requiere que todos los integrantes comprendan claramente los objetivos de dicha asociación y los beneficios mutuos en materia de seguridad que se derivan de dicha colaboración. Algunos de los ámbitos podrían ser: llegar a un acuerdo sobre criterios comunes en materia de ciberseguridad, establecer estructuras de coordinación, procesos y protocolos eficaces de intercambio de información, fomentar la confianza, identificar e intercambiar ideas, planteamientos y prácticas idóneas para mejorar la seguridad y mejorar la coordinación internacional.

Más referencias disponibles en las páginas 63 y 64.

5.5 Esfera prioritaria 5 – Capacitación, creación de competencias y sensibilización

Los debates sobre ciberseguridad pueden estar dominados por consideraciones tecnológicas y políticas, pasando por alto los aspectos humanos fundamentales. En

esta esfera prioritaria se abordan los problemas relacionados con la capacitación en materia de ciberseguridad y la sensibilización de las entidades gubernamentales, los ciudadanos, las empresas y otras organizaciones, que son fundamentales para hacer posible la economía digital en el país.

Entre las buenas prácticas que se examinan en esta sección cabe citar el establecimiento de planes de estudio y programas de sensibilización sobre ciberseguridad, la ampliación de los planes de formación y de los programas de formación profesional, la adopción de planes de certificación internacionales y el fomento de agrupaciones de innovación e investigación y desarrollo (I+D).

5.5.1 Preparación de planes de estudio sobre ciberseguridad

La estrategia debe facilitar la elaboración de planes de estudios con el objetivo de acelerar el desarrollo de las competencias y la sensibilización en materia de ciberseguridad en todo el sistema educativo oficial. Queda comprendida la elaboración de planes de estudios dedicados a la ciberseguridad en las escuelas primarias y secundarias, la integración de cursos de ciberseguridad en todos los programas de informática y de tecnologías de la información de la enseñanza superior y la creación de titulaciones específicas en ciberseguridad y de programas de aprendizaje gubernamentales.

Además, los planes de estudios de las escuelas deben fomentar la sensibilización y estimular el interés por las oportunidades profesionales que ofrece la ciberseguridad. Para promover los esfuerzos en este ámbito, el gobierno también debe considerar la aplicación de diversos sistemas de incentivos, tales como becas para programas de educación privada y subvenciones para aprendizajes relevantes.

5.5.2 Estimular el desarrollo de competencias y la formación profesional

La estrategia debe abordar la elaboración de planes de desarrollo de competencias y formación en materia de ciberseguridad para expertos y no expertos tanto en el sector público como en el privado. Se podría ofrecer formación ejecutiva y operativa, pasantías oficiales y aprendizajes (nacional e internacional) de profesionales de la seguridad, a tenor de las necesidades identificadas por la industria y el gobierno. La formación técnica debe complementarse con iniciativas sobre la gestión de riesgos.

La estrategia también debe fomentar iniciativas destinadas a desarrollar trayectorias profesionales dedicadas a la ciberseguridad, en particular para el sector público, e incentivos para aumentar la oferta de profesionales cualificados en materia de ciberseguridad. Estas iniciativas deben crearse en colaboración con el mundo académico, el sector privado y la sociedad civil. Para eliminar la actual brecha de género de expertos en ciberseguridad, debe considerarse la posibilidad de adoptar un equilibrio de género que motive, aliente y facilite una mayor participación de las mujeres en todas las actividades encaminadas al desarrollo de competencias y formación, garantizando así la inclusión en el futuro.

5.5.3 Ejecutar un programa coordinado de sensibilización sobre ciberseguridad

La estrategia debe asignar la responsabilidad de coordinar campañas y actividades de concienciación sobre la ciberseguridad a escala nacional a una autoridad competente

con el fin de garantizar la racionalización de los recursos y el establecimiento de responsabilidades. La autoridad debe colaborar con las partes interesadas pertinentes para elaborar y aplicar programas de sensibilización sobre ciberseguridad basados en la divulgación de información sobre riesgos y amenazas para la ciberseguridad, así como sobre prácticas idóneas para contrarrestarlos.

El programa de sensibilización en materia de ciberseguridad podría incluir campañas de sensibilización dirigidas a la población en general, a los niños y a los legos en materia digital, programas de educación destinados al consumidor e iniciativas de sensibilización, entre otros, dirigidas a los ejecutivos de los sectores público y privado.

5.5.4 Fomentar la innovación y la I+D en el campo de la ciberseguridad

La estrategia debe fomentar un entorno que estimule la investigación básica y aplicada en materia de ciberseguridad en todos los sectores y en diversos grupos de interesados. Estas iniciativas consisten en, por ejemplo, garantizar que la actividad nacional de investigación esté en consonancia con los objetivos de la estrategia nacional de ciberseguridad; desarrollar programas de I+D sobre ciberseguridad en los organismos públicos de investigación; y difundir eficazmente los nuevos descubrimientos, las tecnologías básicas, las técnicas, los procesos y las herramientas. Por otra parte, los países deben tratar de establecer, en el marco de la estrategia, vínculos con la comunidad internacional de investigación en los ámbitos científicos relacionados con la ciberseguridad, como la informática, la ingeniería eléctrica, las matemáticas aplicadas y la criptografía, pero también en ámbitos no técnicos como las ciencias sociales y políticas, los estudios empresariales y de gestión y la psicología, por citar algunos.

La estrategia debe examinar los mecanismos de incentivos disponibles gracias a subvenciones, contratación pública, créditos fiscales, concursos y otras iniciativas que fomenten el desarrollo de soluciones, productos y servicios innovadores en materia de ciberseguridad.

Más referencias disponibles en las páginas 64 y 65.

5.6 Esfera prioritaria 6 – Legislación y reglamentación

Esta esfera prioritaria comprende la elaboración de un marco jurídico y reglamentario para proteger a la sociedad contra la ciberdelincuencia y promover un entorno cibernético seguro, de conformidad con los principios de inclusión y de entorno de confianza (secciones 4.3 y 4.9, respectivamente). Dicho marco podría incluir: la adopción de legislación que defina lo que constituye ciberactividad ilícita; el reconocimiento jurídico de los derechos individuales y de las libertades civiles; la implantación de mecanismos de observancia; la capacitación necesaria para hacer cumplir el marco; la institucionalización de entidades cruciales; y la cooperación internacional para contrarrestar la ciberdelincuencia.

5.6.1 Promulgar legislación sobre ciberdelincuencia

La estrategia debe promover la instauración de un marco jurídico nacional que defina claramente lo que constituye ciberactividad prohibida y que tenga por objeto reducir la delincuencia en línea. En la mayoría de los casos, este marco adopta la forma de

legislación sobre la ciberdelincuencia, que se materializa promulgando nuevas leyes específicas o enmendando las existentes (por ejemplo, el código penal, las leyes que regulan la banca, las telecomunicaciones y otros sectores).

La estrategia también debe fomentar la creación de un proceso para supervisar la aplicación y revisión de la legislación y los mecanismos de gobernanza, identificar las lagunas y el traslapo de autoridades, y aclarar y priorizar los ámbitos que requieren modernización (por ejemplo, las leyes existentes, como las antiguas leyes de telecomunicaciones).

5.6.2 Reconocer y salvaguardar los derechos y libertades individuales

La estrategia debe salvaguardar las garantías procesales esenciales (en el caso de investigaciones y enjuiciamientos penales), así como los derechos de protección de datos, incluida la protección de la privacidad de los datos personales (posiblemente mediante el desarrollo de un marco de protección de datos y de la privacidad) y de libertad de expresión, con arreglo al principio de los derechos humanos fundamentales (sección 4.5).

5.6.3 Crear mecanismos de observancia

La estrategia debe promover el establecimiento de mecanismos nacionales de observancia (tanto de aplicación como de incentivos). Estos mecanismos deben establecerse para prevenir, combatir y mitigar las acciones dirigidas contra la confidencialidad, la integridad y la disponibilidad de los sistemas e infraestructuras de TIC, así como las amenazas contra los datos informáticos, de conformidad con el marco jurídico antes mencionado. Deben abarcar, entre otras cosas, las particularidades de la investigación digital, la interceptación lícita de las comunicaciones y la utilización de pruebas electrónicas.

5.6.4 Promover la capacitación para la observancia de la ley

La estrategia debe alentar la capacitación para la observancia de la legislación sobre ciberdelincuencia, incluida la capacitación y formación de las diversas partes implicadas en la lucha contra la ciberdelincuencia (por ejemplo, jueces, fiscales, abogados, fuerzas de seguridad, especialistas forenses y otros investigadores). Las fuerzas de seguridad deberían recibir formación especializada para interpretar y aplicar las leyes nacionales sobre ciberdelincuencia (es decir, traducir la ley en conceptos técnicos y viceversa); detectar, disuadir, investigar y enjuiciar eficazmente los delitos cibernéticos; y colaborar eficazmente con la industria y las servicios de seguridad internacionales (por ejemplo, INTERPOL, Europol) para contrarrestar la ciberdelincuencia y fomentar la ciberseguridad. A estos efectos, se debe tener en cuenta la esfera prioritaria 5, relativa a la capacitación, creación de competencias y sensibilización (sección 5.5).

5.6.5 Establecer procesos interinstitucionales

La estrategia debe identificar y reconocer los mandatos de los organismos nacionales con la autoridad principal encargada de la observancia de la legislación en materia de ciberdelincuencia, de los responsables de proteger la infraestructura esencial y de los responsables de garantizar el cumplimiento de todos los requisitos internacionales en

materia de ciberdelincuencia (por ejemplo, garantizar que la legislación nacional esté en consonancia con las obligaciones de los tratados internacionales) y a través de las instancias judiciales (por ejemplo, la cooperación transfronteriza) (véanse también las secciones 5.1.3 y 5.1.4; y la sección 5.6.6).

En algunos ordenamientos jurídicos puede ser necesario promulgar legislación para establecer instituciones que se ocupen de la ciberseguridad, como los EIEI, EIISI y EIII nacionales, o para dar la potestad a un solo organismo de coordinar la política cibernética del país.

5.6.6 Apoyar la cooperación internacional contra la ciberdelincuencia

La estrategia debe demostrar el compromiso de proteger a la sociedad contra la ciberdelincuencia en todo el mundo, mediante la ratificación, siempre que sea posible y de conformidad con la agenda nacional general, de los acuerdos internacionales sobre ciberdelincuencia o acuerdos equivalentes para contrarrestar el delito cibernético, y mediante la promoción de mecanismos de coordinación para hacer frente a la ciberdelincuencia internacional. A tal efecto, puede ser necesario armonizar la legislación nacional con las obligaciones de los tratados internacionales y los acuerdos bilaterales, por ejemplo, mediante el establecimiento de asistencia judicial recíproca, la autorización de investigaciones y enjuiciamientos transfronterizos, la tramitación de pruebas digitales y la extradición. Se debe tomar en consideración la esfera prioritaria 7 sobre cooperación internacional (sección 5.7).

Más referencias disponibles en las páginas 65 y 66.

5.7 Esfera prioritaria 7 – Cooperación internacional

En esta esfera prioritaria se hace hincapié en los aspectos que la estrategia debe abarcar en lo que respecta a los compromisos en materia de ciberseguridad fuera del país, tanto a nivel regional como internacional. La ciberseguridad desempeña cada vez un papel más importante en muy diversos ámbitos de las relaciones internacionales, como los derechos humanos, el desarrollo económico, las transacciones, el comercio, el control de armamentos, la seguridad, la estabilidad, la paz y la resolución de conflictos.

Por lo tanto, la estrategia debe reconocer la naturaleza sin fronteras de la ciberseguridad y destacar la necesidad de cooperar no sólo con los agentes nacionales, sino también con los internacionales. Los compromisos internacionales con los agentes públicos y privados son fundamentales para facilitar un diálogo constructivo, instaurar mecanismos de confianza y cooperación, encontrar soluciones mutuamente aceptables a problemas comunes y crear una cultura mundial de ciberseguridad.

De acuerdo con el principio de enfoque integral y prioridades adaptadas (sección 4.2), la cooperación regional e internacional debe fomentarse en armonía con la estructura política, social, cultural y económica del país, así como con sus prioridades en materia de política exterior.

5.7.1 Reconocer la importancia de la ciberseguridad como prioridad de la política exterior

La estrategia debe manifestar la voluntad de cooperación internacional en materia de ciberseguridad y reconocer que los problemas cibernéticos son parte integrante de la política exterior del país. Con este fin, es importante fomentar el desarrollo y la utilización de competencias y aptitudes sobre asuntos cibernéticos (ciberdiplomacia) para complementar los métodos y procesos tradicionales de la diplomacia. La estrategia también puede incluir la creación de estructuras orgánicas específicas y el establecimiento de oficinas especializadas o de personal formado dedicadas principalmente a la diplomacia en asuntos cibernéticos.

Más concretamente, la estrategia debe articular claramente las esferas prioritarias del gobierno y los objetivos a largo plazo para la cooperación internacional, incluyendo qué agentes (por ejemplo, públicos, privados, regionales, globales) estarían involucrados. Podrían estipular, por ejemplo, el apoyo al establecimiento de normas internacionales de ciberseguridad y medidas de fomento de la confianza, el compromiso con el fomento de la capacidad en materia de ciberseguridad, la participación en la elaboración de normas internacionales de ciberseguridad y la adhesión a los instrumentos regionales e internacionales existentes.

Quizá también sea necesario mejorar la armonización entre los diferentes actores gubernamentales (por ejemplo, el jefe de Estado y el gabinete, el Ministerio de Asuntos Exteriores, el Ministerio de TIC, el Ministerio de Industria y Comercio, el Ministerio de Justicia, el Ministerio de Defensa, etc.), de modo que la posición política expresada por un actor nacional en una mesa de negociación en el ámbito de la ciberseguridad internacional esté adecuadamente coordinada y armonizada con otros organismos gubernamentales.

5.7.2 Participar en debates internacionales

La estrategia debe identificar foros y mecanismos de cooperación internacionales específicos a los que el país desee adherirse para participar en asuntos diplomáticos relacionados con la ciberseguridad. Por ejemplo, organizaciones regionales o mundiales, debates intergubernamentales, alianzas entre los sectores público y privado, así como mecanismos tradicionales de cooperación y colaboración que incluyan cuestiones de ciberseguridad.

A medida que el país comience a participar en estos debates, es probable que el gobierno tenga que desarrollar competencias y habilidades adicionales relacionadas con asuntos cibernéticos y aumentar su capacidad general en materia de ciberseguridad. Por consiguiente, es importante dar prioridad a estos esfuerzos y asignar los recursos adecuados (humanos y económicos) para garantizar la obtención de resultados concretos.

5.7.3 Promover la cooperación oficial y oficiosa en el ciberespacio

La estrategia debe indicar los mecanismos operativos de cooperación internacional con los que el país desea comprometerse. Quizá el país desee participar en iniciativas internacionales oficiales y oficiosas que promuevan la cooperación, por ejemplo, en la elaboración de políticas y leyes, la aplicación de la ley, la respuesta a incidentes y el intercambio de información y amenazas. La participación en tales iniciativas

podría, por ejemplo, mejorar la cooperación y el intercambio de información entre las autoridades pertinentes sobre amenazas y vulnerabilidades potenciales.

5.7.4 Armonizar los esfuerzos nacionales e internacionales en materia de ciberseguridad

La estrategia debe tener en cuenta las iniciativas regionales e internacionales existentes en materia de ciberseguridad y fomentar su armonización y avenencia. De este modo el país podrá aprovechar las prácticas idóneas existentes y contribuir a la cohesión y convergencia de los planteamientos en materia de ciberseguridad.

Con este fin, la estrategia debe mostrar el compromiso del país de garantizar la coherencia entre sus programas de política interior y exterior armonizando su marco jurídico y sus políticas nacionales con sus compromisos internacionales, y sus planteamientos nacionales en materia de ciberseguridad con sus esfuerzos internacionales.

Algunos ejemplos notables de los esfuerzos internacionales existentes que podrían considerarse como parte de la estrategia son, entre otros: la labor del Grupo de Expertos Gubernamentales de las Naciones Unidas sobre los avances en la esfera de la información y las telecomunicaciones en la esfera de la seguridad internacional (GEG de las Naciones Unidas), la Organización para la Seguridad y la Cooperación en Europa (OSCE) sobre medidas de fomento de la confianza (MFC) y normas internacionales aplicables en el ciberespacio, la labor del Subgrupo de delincuencia de alta tecnología del grupo de los siete, el Convenio de Budapest sobre la Ciberdelincuencia del Consejo de Europa, la Convención de la Unión Africana sobre ciberseguridad, el acuerdo entre los gobiernos de los Estados miembros de la Organización de Cooperación de Shanghái sobre cooperación en materia de seguridad internacional de la información, la Convención árabe de lucha contra los delitos relacionados con la tecnología de la información, la Directiva de la CEDEAO relativa a la lucha contra la ciberdelincuencia, así como el apoyo del Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCDCOE OTAN) a los Manuales de Tallin 1.0 y 2.0.

Más referencias disponibles en la página 66.

6 Material de referencia

En el proceso de elaboración de esta guía, se hizo un inventario de las guías existentes y de las mejores prácticas.

Esto nos permitió identificar material ya disponible que sirva de ayuda a los países a la hora de elaborar su estrategia nacional de ciberseguridad. La lista que figura a continuación ofrece un catálogo completo del material mencionado, con enlaces a sitios web.

CCI (2017), *Harare Scheme on Mutual Legal Assistance in Criminal Matters*

Carnegie Mellon (2003), *Handbook for Computer Security Incident Response Teams (CSIRTs)*

Commonwealth (2018), *Commonwealth Cyber Declaration*

CTO (2015), *Commonwealth Approach for Developing National CyberSecurity Strategies*

Consejo de Europa (2001), *Convenio de Budapest sobre la Ciberdelincuencia*

Council of the European Union (2017), Cyber Diplomacy toolbox

ENISA (2014), *An Evaluation Framework For National Cyber Security Strategies*

ENISA (2011), *CERT Operational Gaps and Overlaps*

ENISA (2011), *Good Practice Guide for Incident Management*

ENISA (2015), *Methodologies for the Identification of Critical InformationInfrastructure Assets and Services*

ENISA (2016), *National Cyber Security Strategy Good Practice Guide – Designing and Implementing National Cyber Security Strategies*

ENISA (2012), *National Cyber Security Strategies: Practical Guide on Development and Execution*

ENISA (2012), *National Cyber Security Strategy, Setting the Course for National Efforts to Strengthen Security in Cyberspace*

ENISA (2016), *National Cyber Security Strategies: Training Tool*

ENISA (2016), *Stocktaking, Analysis and Recommendations on the Protection of CIIs*

ENISA (2016), *Strategies for Incident Response and Cyber Crisis Cooperation*

Global Cyber Security Capacity Centre, University of Oxford (2016), *Cybersecurity Capacity Maturity Model for Nations*

UIT (2017), *Seguridad en las redes de información y comunicación: Prácticas óptimas para el desarrollo de una cultura de ciberseguridad*

UIT (2017), *Índice de ciberseguridad mundial (GCI)*

UIT (2011), *Guía de estrategias nacionales en materia de ciberseguridad*

UIT (2010), *Entender el ciberdelito: Fenómenos, retos y respuesta legal*

UIT (2009), *Guía sobre ciberseguridad para los países en desarrollo*

Microsoft (2013), *Developing a National Strategy for Cybersecurity*

Microsoft (2014), *Critical Infrastructure Protection: Concepts and Continuum*

Microsoft (2014), *Critical Connections: Protecting Infrastructures*

Microsoft (2014), Hierarchy of Cybersecurity Needs

Microsoft (2018), Building an effective national cybersecurity agency

Microsoft (2018), *Cybersecurity Policy Framework*

Microsoft (2015), *Information Sharing Framework for Cybersecurity*

Microsoft (2017), *Risk Management for Cybersecurity: Security Baselines*

CCDCOE OTAN (2012), *National Cyber Security Framework Manual*

CCDCOE OTAN (2013), *National Cyber Security Strategy Guidelines*

NIST (2014), *Framework for Improving Critical Infrastructure Cybersecurity*

OAS (2015), *Best Practice for Establishing a National CSIRT*

OAS (2004), *Comprehensive Inter-American Cybersecurity Strategy: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity*

OAS (2015), *Cyber Security Awareness Campaign Toolkit*

OAS (2015), *Report Cybersecurity and Critical Infrastructure in the Americas*

OCDE (2015), *Companion Document to the Recommendation on Digital Security Risk Management for Economic and Social Prosperity*

OCDE (2012), *Cybersecurity Policy Making at a Turning Point*

OCDE (2015), *Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity*

OCDE (2013), *Recommendation of the Council Concerning Guidelines for the Protection of Privacy and Transborder Flows of Personal Data (Privacy Guidelines)*

OCDE (2008), *Recommendation of the Council on the Protection of Critical Information Infrastructures*

OCDE (2007), *Report on the Development of Policies for the Protection of Critical Information Infrastructures*

Potomac Institute for Policy Studies (2015), *Cyber Readiness Index 2.0 – A Plan for Cyber Readiness: A Baseline and An Index*

Naciones Unidas (2015), *Sustainable Development Goals*

Naciones Unidas (1976), *Pacto Internacional de Derechos Económicos, Sociales y Culturales, Pacto Internacional de Derechos Civiles y Políticos y Protocolo Facultativo del Pacto Internacional de Derechos Civiles y Políticos, Resolución 2200 (XXI)*

Naciones Unidas (2014), *El derecho a la privacidad en la era digital, Resolución A/RES/68/167*

Naciones Unidas (1948), *Declaración Universal de Derechos Humanos*

UNCTAD (2014), *A Framework for Information and Communications Technology Policy Reviews*

UNCTAD, *Developing E-Commerce Legislation*

UNCTAD (2016), *Study on Data Protection Regulations and International Data Flows*

UNHR (1976), *International Covenant on Civil and Political Rights*

World Bank et al (2017), *Combatting Cybercrime: Tools and Capacity Building for Emerging Economies*

A continuación se desglosan las referencias para cada uno de los principios y buenas prácticas.

Ciclo de vida de la estrategia nacional de ciberseguridad

Subtema	Referencias
Iniciación	ENISA (2016), National Cyber Security Strategies: Training Tool CCDCOE OTAN (2013): National Cyber Security Strategy Guidelines, section: 1.3
Inventario y análisis	ENISA (2016), National Cyber Security Strategies: Training Tool CCDCOE OTAN (2013): National Cyber Security Strategy Guidelines, sections: 2.1, 2.2, 3.2.1, 3.3.1 CCDCOE OTAN (2012): National Cyber Security Framework Manual, sections: 3.4, 4
Elaboración de la estrategia nacional	ENISA (2016), National Cyber Security Strategies: Training Tool
Ejecución	ENISA (2016), National Cyber Security Strategies: Training Tool
Supervisión y evaluación	ENISA (2016), National Cyber Security Strategies: Training Tool CCDCOE OTAN (2013): National Cyber Security Strategy Guidelines, section: 3.9 CCDCOE OTAN (2012): National Cyber Security Framework Manual, section: 2.4

Principios generales

Subtema	Referencias
Visión	Microsoft (2013), Developing a National Cybersecurity Strategy, p.4
	CCDCOE OTAN (2013): National Cyber Security Strategy Guidelines, section: 1.3.1
	OCDE (2015), Recommendation on Digital Security Risk Management for Economic and Social Prosperity
	Potomac Institute for Policy Studies (2015), Cyber Readiness Index 2.0 – A Plan for Cyber Readiness: A Baseline and an Index, p.1-3
Enfoque integral y prioridades adaptadas	ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies
	Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations(C-MM), Dimension 1.1, p.14
	Microsoft (2013), Developing a National Cybersecurity Strategy, p.5
Inclusividad	CCI (2013), Checklist p2
	CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies 4.5 and 4.6.6
	ENISA (2015), Methodologies for the Identification of Critical Information Infrastructure Assets and Services, chapter 3
	ENISA (2016), An Evaluation Framework for National Cyber Security Strategies 3.2
	ENISA (2016), National Cyber Security Strategies: Setting the Course for National Efforts to Strengthen Security in Cyberspace, p.9
	Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.1, p.14
	UIT (2011), Guía para la elaboración de una estrategia nacional de ciberseguridad, sección 5.3
	CCDCOE OTAN (2013): National Cyber Security Strategy Guidelines, section: 1.1.3
	CCDCOE OTAN (2012): National Cyber Security Framework Manual, sections: 3.4, 3.5, 4.3
	OAS (2015), Cyber Security Awareness Campaign Toolkit, p.20
	OAS (2015), Report on Cybersecurity and Critical Infrastructure in the Americas, p.2

Subtema	Referencias
Inclusividad (cont.)	OCDE (2015), Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, p.14-15
	OCDE (2013), Recommendation of the Council Concerning Guidelines for the Protection of Privacy and Transborder flows of Personal Data (Privacy Guidelines); Supplementary Explanatory Memoran-dum to the Revised OCDE Privacy Guidelines, p.31
	Potomac Institute for Policy Studies (2015), Cyber Readiness Index 2.0 – A Plan for Cyber Readiness: A Baseline and an Index, p.3-6
	UNCTAD (2016), Data Protection Regulations and International Data Flows: Implications for Trade and Development
	UNCTAD (2014), A Framework for Information and Communications Technology Policy Reviews
Prosperidad económica y social	Microsoft (2014), Hierarchy of Cybersecurity Needs, chapter 1
	CCDCOE OTAN (2012): National Cyber Security Framework Manual, sections: 1.5.1, 2.2.1
	Potomac Institute for Policy Studies (2015), Cyber Readiness Index 2.0 – A Plan for Cyber Readiness: A Baseline and an Index, p.1-3
Derechos humanos fundamentales	CCI (2013), Checklist 2.6.5.
	CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies, Principle 4
	ENISA (2014), An Evaluation Framework for Cyber Security Strategies, 3.1.1 Objectives
	Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 4.1, p.39
	UIT (2011), Guía de estrategias nacionales en materia de ciberseguridad, sección 7.4
	Microsoft (2013), Developing a National Cybersecurity Strategy, p.5
	CCDCOE OTAN (2013): National Cyber Security Strategy Guidelines, sections: 1.3.1, 1.3.3
	CCDCOE OTAN (2012): National Cyber Security Framework Manual, sections: 1.5.4, 1.5.5, 5.2.6
	OCDE (2015), Companion Document to the Recommendation on Digital Security Risk Management for Economic and Social Prosperity, principle 9 and principle 3

Subtema	Referencias
Derechos humanos fundamentales (cont.)	UNCTAD (2016), Data Protection Regulations and International Data Flows: Implications for Trade and Development Naciones Unidas (1948), Declaración Universal de Derechos Humanos Naciones Unidas (1976), Pacto Internacional de Derechos Económicos, Sociales y Culturales, Pacto Internacional de Derechos Civiles y Políticos y Protocolo Facultativo del Pacto Internacional de Derechos Civiles y Políticos Naciones Unidas (2014), El derecho a la privacidad en la era digital
Gestión de riesgos y resiliencia	ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.3, p.15 Microsoft (2013), Developing a National Cybersecurity Strategy, p.6 Microsoft (2017), Risk Management for Cybersecurity: Security Baselines OCDE (2015), Recommendation on Digital Security Risk Management Economic and Social Prosperity and Companion Document
Conjunto adecuado de instrumentos políticos	ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies CCDCOE OTAN (2013): National Cyber Security Strategy Guidelines, section: 3.1 CCDCOE OTAN (2012): National Cyber Security Framework Manual, section: 1.4
Dirigentes, funciones y atribución de recursos claramente definidos	ENISA (2016), NCSS Good Practice Guide – Designing and Implementing National Cyber Security Strategies CCDCOE OTAN (2012): National Cyber Security Framework Manual, section: 4 Microsoft (2018):Building an effective national cybersecurity agency Potomac Institute for Policy Studies (2015), Cyber Readiness Index 2.0 – A Plan for Cyber Readiness: A Baseline and an Index, sections: 1-7

Subtema	Referencias
Entorno de confianza	Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 2.2, p.25 CCDCOE OTAN (2013): National Cyber Security Strategy Guidelines, section: 1.3.1 Potomac Institute for Policy Studies (2015), Cyber Readiness Index 2.0, sections: 4, 6

Buenas prácticas en la estrategia nacional de ciberseguridad

Subtema	Referencias
Esfera prioritaria 1 – Gobernanza	CCI (2013), Checklist. CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies, sections: 4.4.1, 4.4.4, 4.4.5, 4.4.8, 4.4.9, 4.4.20, 4.4.21, 4.4.34, 4.5 ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies, sections: 3.1, 3.2, 3.4, 3.5, 3.17 ENISA (2016), An Evaluation Framework for National Cyber Security Strategies, sections: 2.2.1, 3.1.1, 3.1.2, 3.1.3 ENISA (2016), National Cyber Security Strategies: Setting the course for National Efforts to Strengthen Security in Cyberspace, sections: 4, 6 Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.1, 1.5, 1.6, p.14-15 UIT (2011): Guía para la elaboración de una estrategia nacional de ciberseguridad, secciones: 5.2.1, 5.3, 7.2, 7.3, 11.1, 11.2, 20, 20.2 Microsoft (2013), Developing a National Cybersecurity Strategy, sections: A Principled Approach to Cybersecurity, Establishing Clear Priorities and Security Baseline Microsoft (2018) Building an effective national cybersecurity agency CCDCOE OTAN (2013), National Cyber Security Strategy Guidelines, sections: 1.1, 3.3, 3.8 CCDCOE OTAN (2012), National Cyber Security Framework Manual, sections: 1.4.2, 2.1.1 2.1.3, 2.2, 2.3, 2.4, 3.1, 3.5, 4, 5.3.1 OCDE (2012), Cybersecurity Policy Making at a Turning Point, Annex IV OCDE (2013), Recommendation of the Council Concerning Guidelines for the Protection of Privacy and Transborder Flows of Personal Data (Privacy Guidelines) OCDE (2015), Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, 2-A, Companion Document

Subtema	Referencias
Esfera prioritaria 1 – Gobernanza (cont.)	OCDE (2015), Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, 2-A, Companion Document OCDE (2008), Recommendation of the Council on the Protection of Critical Information Infrastructures Potomac Institute for Policy Studies (2015), Cyber Readiness Index 2.0, section 1
Esfera prioritaria 2 – Gestión de riesgos en la ciberseguridad nacional	CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies, sections: 4.4.6, 4.4.15, 4.4.24, 4.4.25, 4.4.26, 4.4.27 ENISA (2016), National Cyber Security Strategy Good Practice Guide – Designing and Implementing National Cyber Security Strategies, section: 3.3 Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.3, p.14 UIT (2011), Guía para la elaboración de una estrategia nacional de ciberseguridad, sección 10.1.2 Microsoft (2017), Risk Management for Cybersecurity: Security Baselines Microsoft (2013), Developing a National Cybersecurity Strategy, chapter on Building a Risk Approach CCDCOE OTAN (2013), National Cyber Security Strategy Guidelines, section: 3.5 CCDCOE OTAN (2012): National Cyber Security Framework Manual, sections: 2.1.2, 5.3.2 NIST (2015), Framework for Improving Critical Infrastructure Cybersecurity OAS (2018), Managing National Cyber Risk OCDE (2008), Recommendation of the Council on the Protection of Critical Information Infrastructures OCDE (2015), Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity Potomac Institute for Policy Studies (2015), Cyber Readiness Index 2.0, section: 1

Subtema	Referencias
Esfera prioritaria 3 – Preparación y resiliencia	Carnegie Mellon (2003), Handbook for Computer Security Incident Response Teams (CSIRTs)
	CCI (2013), Checklist
	CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies, section: 4.4.3, 4.4.20, 4.4.21, 4.4.22, 4.4.27, 4.4.31
	ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies, sections: 3.6, 3.7, 3.10, 3.14, 4.1, 4.5, 4.8
	ENISA (2016), Strategies for Incident Response and Cyber Crisis Cooperation, p.
	ENISA (2011), CERT Operational Gaps and Overlaps, p.
	ENISA (2011), Good Practice Guide for Incident Management, p.
	Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.2, p.14
	UIT (2011), Guía para la elaboración de una estrategia nacional de ciberseguridad: 11.3, 17.3
	Microsoft (2017), Risk Management for Cybersecurity: Security Baselines
	Microsoft (2015), Information Sharing Framework for Cybersecurity
	Microsoft (2013), Developing a National Strategy for Cybersecurity, section: Building Incident Response Capabilities
	CCDCOE OTAN (2013): National Cyber Security Strategy Guidelines, Section: 3.5
	CCDCOE OTAN (2012): National Cyber Security Framework Manual, sections: 3.2, 4.2.2
	OAS (2016), Best Practice for Establishing a National CSIRT, p.35
	OAS (2004), Comprehensive Inter-American Cybersecurity Strategy: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity, pp.3-4
	OCDE (2015), Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, section: 2-B
	Potomac Institute for Policy Studies (2015), Cyber Readiness Index 2.0, sections: 2, 4

Subtema	Referencias
Esfera prioritaria 4 – Servicios de infraestructura esencial y servicios fundamentales	CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies, sections: 4.4.12, 4.4.13,4.4.20, 4.4.25, 4.4.26, 4.4.28, 4.4.32 Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.3, 1.4, p.14; Dimension 5.2, p.49 ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies, section: 3.6 ENISA (2015), Methodologies for the Identification of Critical Information Infrastructure Assets and Services ENISA (2016), An Evaluation Framework for National Cyber Security Strategies, section: 4.2 UIT (2011), Guía para la elaboración de una estrategia nacional de ciberseguridad, secciones: 5.1.1, 5.3.3, 11.4 Microsoft (2017), Risk Management for Cybersecurity: Security Baselines Microsoft (2014), Critical Infrastructure Protection: Concepts and Continuum, all sections Microsoft (2014), Critical Connections: Protecting Infrastructures, all sections CCDCOE OTAN (2013): National Cyber Security Strategy Guidelines, sections: 3.4, 3.5 CCDCOE OTAN (2012), National Cyber Security Framework Manual, section: 4.5.4 OAS (2015), Report Cybersecurity and Critical Infrastructure in the Americas OCDE (2015), Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity OCDE (2008), Recommendation of the Council on the Protection of Critical Information Infrastructures: Part I, Part II Potomac Institute for Policy Studies (2015): Cyber ReadinessIndex 2.0, sections: 2, 4

Subtema	Referencias
Esfera prioritaria 5 – Capacitación, creación de competencias y sensibilización	CCI (2013), Checklist; CCI (2005, 2017), Commonwealth Network of Contact Persons Framework; CCI (2011), Harare Scheme on Mutual Legal Assistance in Criminal Matters; CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies, sections: 4.4.11, 4.4.17, 4.4.20, 4.4.34, 4.4.12, 4.4.14, 4.4.16, 4.4.23 ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies, sections: 3.12, 3.8, 3.11, 3.13, 4.3, 4.6, 4.7, 4.14 ENISA (2016), Strategies for Incident Response and Cyber Crisis Cooperation, section: 2.1 ENISA (2011), CERT Operational Gaps and Overlaps, p.6, 16, 19, 21, 27, 29, 31, 32, 50, 57 ENISA (2010), Good Practice Guide for Incident Management, p.19, 23, 26, 32, 46, 56, 58, 64, 69 Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.5, p.15; Dimension 2.1, 2.2., 2.3, p.25; Dimension 3-1, 3-2, 3-3, p. 32; Dimension 5.6, p.49 UIT (2011), Guía para la elaboración de una estrategia nacional de ciberseguridad, secciones: 5.3.7, 5.3.8, 12.4, 12.1, 12.3, 18 Microsoft (2013), Developing a National Strategy for Cybersecurity, section: Driving Research and Technology Investment, Public Awareness, Workforce Training and Education; CCDCOE OTAN (2013, National Cyber Security Strategy Guidelines, section: 3.5CCDCOE OTAN (2012), National Cyber Security Strategy Framework Manual, sections: 4.5.5, 4.6.3; OAS (2015), Cyber Security Awareness Campaign Toolkit, all sections; OCDE (2015), Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, section: 2-B Potomac Institute for Policy Studies (2015), Cyber Readiness Index 2.0, sections: 2, 5 UNCTAD (2015), Programme on E-Commerce and Law Reform

Subtema	Referencias
Esfera prioritaria 6 – Legislación y reglamentación	CCI (2013), Checklist
	CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies, sections: 4.4.5, 4.4.6, 4.4.7, 4.4.8, 4.4.9, 4.4.18, 4.4.19, 4.4.20
	Consejo de Europa (2001), Convenio de Budapest sobre la Ciberdelincuencia, articulo 15
	ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies, sections: 3.15, 3.184.9, 4.12
	Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 4.1, 4.2, 4.3, p.39-40; Dimension 5.7, p.50
	UNHR (1976), International Covenant on Civil and Political Rights, article 19
	UIT (2011), Guía para la elaboración de una estrategia nacional de ciberseguridad, secciones: 5.3.4, 5.3.5, 9, 11.5, 12.2, 15
	UIT (2010), UIT Toolkit for Cybercrime Legislation
	CCDCOE OTAN (2013), National Cyber Security Strategy Guidelines, section: 3.2
	CCDCOE OTAN (2012), National Cyber Security Strategy Framework Manual, section: 5
	OAS:
	Potomac Institute for Policy Studies (2015), Cyber Readiness Index 2.0, section: 3
	ONU (2015), Sustainable Development Goals, article 16.3
	UNCTAD, Global Cyberlaw Tracker
	World Bank et al., Combatting Cybercrime: Tools and Capacity Building for Emerging Economies

Subtema	Referencias
Esfera prioritaria 7 – Cooperación internacional	CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies, sections: 4.4.20, 4.4.21 ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies, sections: 3.16 and 4.10 ENISA (2016), Guidebook on National Cyber Security Strategies, section: 3.16 Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 4.3, p.40 UIT (2011), Guía para la elaboración de una estrategia nacional de ciberseguridad, secciones: 5.3.9, 10.2.2, 13, 19 Microsoft (2013), Developing a National Strategy for Cybersecurity, section on structuring international engagement CCDCOE OTAN (2013), National Cyber Security Strategy Guidelines, sections: 1.3, 3.2.1, 3.3.2 CCDCOE OTAN (2012), National Cyber Security Strategy Framework Manual, sections: 4.7, 5.4.2, 5.4.3 OCDE (2008), Recommendation of the Council on the Protection of Critical Information Infrastructures, chapters: 4, 5 OCDE (2015), Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, p. 13, 48, 58 Potomac Institute for Policy Studies (2015), Cyber Readiness Index 2.0, sections: 4, 6

7 Acrónimos

Acrónimo	Definición
CCI	Iniciativa de la Commonwealth contra el Delito Cibernético
EIEI	Equipo de intervención en caso de emergencia informática
MFC	Medidas de fomento de la confianza
IEI	Infraestructura esencial de la información
CTO	Organización de Telecomunicaciones de la Commonwealth
ENISA	Agencia de la Unión Europea para la Seguridad de las Redes y de la Información
TIC	Tecnologías de la información y la comunicación
UIT	Unión Internacional de Telecomunicaciones
CCDCOE OTAN	Centro de Excelencia en Ciberdefensa Cooperativa de la OTAN
NIST	Instituto Nacional de Normas y Tecnología
OEA	Organización de los Estados Americanos
OCDE	Organización para la Cooperación y el Desarrollo Económicos
ONU	Naciones Unidas
UNCTAD	Conferencia de las Naciones Unidas sobre Comercio y Desarrollo

ISBN: 978-92-61-27793-2