COMITÉ 5G

ift INSTITUTO FEDERAL DE TELECOMUNICACIONES

GUÍA PARA DESARROLLAR UNA ESTRATEGIA DE CIBERSEGURIDAD NACIONAL

Recomendaciones y directrices para la integración de un Marco Regulatorio Nacional de Ciberseguridad en México.

Comité Técnico en Materia de Despliegue de 5G en México

Mesa 5. Ciberseguridad

Glosario

Acrónimos

Acrónimo	Término
Estrategia	Estrategia Nacional de Ciberseguridad
IC	Infraestructuras Críticas
ICI	Infraestructuras Críticas de Información
ONU	Organización de las Naciones Unidas
TIC	Tecnologías de la Información y Comunicación
UIT	Unión Internacional de Telecomunicaciones

Contenido

1. Introducción

Durante los últimos años hemos visto el vertiginoso uso de la Internet comercial, que plantó la semilla de una red interconectada y una red digital global, que se ha convertido en un eje primordial de nuestra conexión al mundo digital, de la que hacemos uso de manera cotidiana en una gran diversidad de actividades y sectores usuarios. El ciberespacio es un nuevo dominio estratégico, diferente al territorio físico que conocemos. Gradualmente se ha convertido en el sistema nervioso a través del cual opera la sociedad. Actualmente, los países van reconociendo la gran importancia e incursionando en el desarrollo de las tecnologías en el ciberespacio. El avance de las redes ha ayudado a impulsar el progreso económico y social. Las redes abiertas han fomentado el flujo y el intercambio de información, han propiciado mayores oportunidades para la innovación, la reducción de costos de transacciones y servicios, han contribuido a mejorar la salud de la población, y a generar riqueza en el mundo.

La evolución de las redes interconectadas ha incentivado la inversión y permitido nuevos modelos de consumo lo que ha impulsado el crecimiento económico global. Así, las redes abiertas conectan el mundo, facilitando los intercambios económicos entre regiones y promoviendo el comercio global. Con el crecimiento exponencial en la generación, recolección y análisis de información, aunado al uso de tecnología de punta que nos permite acceder a canales de comunicación con grandes capacidades, es necesario analizar desde una perspectiva holística la transferencia masiva de datos y las tecnologías asociadas, con plena conciencia de las complejidades, retos y riesgos que también se generan, de manera simultánea, y que crean vulnerabilidades, riesgos y amenazas intrínsecas a la operación de los sistemas mismos.

A pesar de los grandes beneficios personales, sociales y empresariales derivados de la transformación digital y la accesibilidad a través de medios virtuales, se crea una brecha de alta relevancia para atender los riesgos inherentes. La confidencialidad, la integridad y la disponibilidad de la infraestructura de las Tecnologías de la Información y Comunicación (TIC) se ven amenazadas por riesgos que evolucionan rápidamente, como el robo o uso inadecuado de información personal y sensible, amenazas a infraestructuras críticas, riesgos en la operación comercial, etc.

Respecto de la seguridad de infraestructura y datos, la tecnología digital tiene vulnerabilidades que emanan de su naturaleza física (debilidades intrínsecas o físicas) y de la interacción con los seres humanos (ingeniería social). La importancia de estas vulnerabilidades crece en la medida en que nuestras sociedades adoptan la tecnología digital para la realización de actividades cotidianas. Se trata de la paradoja de la innovación, que ofrece grandes beneficios a la sociedad, pero no completamente exentos de riesgo. La confidencialidad, la integridad y la disponibilidad de la infraestructura de las TIC se ven amenazadas por riesgos que evolucionan rápidamente.

Para aprovechar plenamente el potencial de la tecnología, los Estados deben alinear sus visiones de desarrollo tecnológico, económico y de bienestar social, las cuales son parte de la obligación del Estado en materia de seguridad nacional. La ciberseguridad es un dominio o materia que debe servir como una plataforma habilitante para mitigar los riesgos de seguridad asociados a la proliferación de infraestructuras y aplicaciones que operan sobre redes digitales, las cuales se deben combatir con estrategias nacionales integrales de ciberseguridad y planes de resiliencia, de modo que los países estén en condiciones de perseverar en el crecimiento económico y los objetivos de desarrollo nacional, incluyendo las estrategias de seguridad nacional que persiguen.

Los Estados deben ser muy asertivos en la delimitación, definición y aplicación de varios conceptos que suelen usarse en ocasiones como sinónimos y que puede generar problemas al momento de su aplicación, referencia, discusión y definición. Así, la ciberseguridad se dedica a salvaguardar sistemas, aplicaciones, datos y redes contra amenazas cibernéticas (por ejemplo, inutilizar sistemas de gestión mediante el uso de programas computacionales invasivos) y violaciones de la privacidad. Con el aumento exponencial de datos y de información almacenada en formato digital y la multiplicación de servicios y productos a través de Internet, la importancia de proteger los activos digitales se ha vuelto crítica.

a) Ciberseguridad, ciberdelito, ciberterrorismo y ciber inteligencia

La ciberseguridad se refiere al "conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno"[1]. Así, mediante las medidas de ciberseguridad, se busca garantizar la integridad, confidencialidad y disponibilidad de la información almacenada, procesada, generada o transferida a través de entornos digitales.

El ciberdelito abarca actividades delictivas y penales llevadas a cabo en línea, que pueden amenazar activos digitales o que también se puede referir a un término más amplio que engloba cualquier actividad criminal que involucre el uso de tecnologías de la información y comunicación, ya sea directa o indirectamente para cometer un delito, incluyendo tanto aquellos que tienen como objetivo a las infraestructuras tecnológicas como aquellos que utilizan estas tecnologías para facilitar otros delitos. Es recomendable en este campo seguir el Proyecto de convención de las Naciones Unidas contra la ciberdelincuencia[2].

En cuanto al ciberterrorismo, se trata del "empleo del ciberespacio como fin o medio para generar terror o pánico generalizado, con la finalidad de influir en las decisiones o imponer ideologías contra la sociedad y/o las instituciones de un Estado- Nación"[3]. Implica el uso de la tecnología informática para realizar actos terroristas, los cuales son clasificados por la legislación de cada país, sin embargo, su finalidad es causar pánico, interrupción y daño a gran escala mediante la manipulación no autorizada de sistemas digitales.

La ciber inteligencia consiste en la actividad de recopilación, análisis y recomendaciones o requerimientos para la detección y respuesta defensiva en las organizaciones relacionadas con amenazas cibernéticas. Su propósito es proporcionar información, conocimientos y capacidades para mejorar la postura de seguridad y responder eficazmente a las amenazas digitales, contribuyendo así a la prevención de posibles ataques en la red. Las Secretarías de la Defensa

[1] Disponible en: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136&lang=es
[2] Disponible en: https://documents.un.org/doc/undoc/gen/v24/055/09/pdf/v2405509.pdf
[3] Disponible en: https://www.gob.mx/cms/uploads/attachment/file/936056/GLOSARIO_TERMINOS_2024.pdf

Nacional y de Marina la definen como la *"Disciplina de la inteligencia que utiliza el Ciberespacio como medio para adquirir, analizar y utilizar información valiosa relacionada con amenazas que pueden afectar a organizaciones o tener un impacto en la Seguridad Nacional. Este proceso involucra la recopilación y análisis de datos y la identificación de amenazas, con el propósito de apoyar al Estado-Nación, incluyendo las Fuerzas Armadas, en todos los ámbitos operacionales (tierra, mar, aire, espacio y Ciberespacio)"*[4].

En síntesis, la ciberseguridad busca salvaguardar la integridad de los sistemas; el ciberdelito se enfoca en actividades criminales en línea; el ciberterrorismo involucra actos terroristas digitales; y la ciber inteligencia se dedica a la recopilación y análisis de información para prevenir y mitigar amenazas cibernéticas. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el entorno digital. Las propiedades de seguridad incluyen una o más de las siguientes: **disponibilidad; integridad, que puede incluir la autenticidad y el no repudio; confidencialidad.**

En este contexto, ha ganado relevancia el concepto de **Estrategia Nacional de Ciberseguridad,** el cual hace referencia a un plan integral y de alto nivel en la jerarquía de las administraciones públicas desarrollado para proteger los sistemas, las infraestructuras críticas y los intereses de los ciudadanos como respuesta a las amenazas cibernéticas. Este plan debe contemplar políticas, principios, objetivos y acciones específicas que se enfoquen en garantizar la seguridad, resiliencia y protección de los sistemas de información y comunicación del país. La estrategia deberá considerar la gestión de una amplia gama de riesgos y buscar coordinar los esfuerzos de diversas entidades públicas y privadas para fortalecer la seguridad nacional en el entorno digital.

Dada la complejidad de estas estrategias, es pertinente desarrollar una guía para su diseño, de manera tal que se aborde integralmente la problemática asociada a la ciberseguridad.

Dada la complejidad del ciberdelito y la evolución de los ciberataques, la estrategia nacional de ciberseguridad considera dar forma a las directrices estratégicas del enfoque de ciberseguridad de un país y desempeña un papel crucial en su política de protección de bienes y servicios digitales. Sus principios se deben contemplar en la adecuación del marco legislativo de ciberseguridad nacional y debe basarse en una comprensión y un análisis globales del entorno digital general, al tiempo que debe adaptarse a las circunstancias y prioridades específicas de México.

El presente documento integra la visión, recomendaciones y conocimiento de organizaciones intergubernamentales, empresas del sector privado, operadores, así como de la academia y de la sociedad civil que integran la Mesa 5 del Comité Técnico en materia de despliegue de 5G en México, y tiene como objetivo apoyar a los líderes nacionales y a los diseñadores de políticas y regulaciones en la materia en el desarrollo de respuestas, tanto defensivas como proactivas, a los riesgos cibernéticos. Se pretende ofrecer un conjunto estructurado de recomendaciones para actualizar la Estrategia Nacional de Ciberseguridad expedida en 2017[5]. Asimismo, el documento toma como insumo las recomendaciones de la Unión Internacional de Telecomunicaciones (UIT) desarrolladas

[4] Disponible en: https://www.gob.mx/cms/uploads/attachment/file/936056/GLOSARIO_TERMINOS_2024.pdf
[5] Disponible en: www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

en la Guía para la Elaboración de una Estrategia Nacional de Ciberseguridad, así como una serie de documentos estratégicos sobre la materia elaborados por el Foro Económico Mundial.

En este documento se define la ciberseguridad como el conjunto de herramientas, políticas, directrices, enfoques de gestión de riesgos, acciones, capacitaciones, mejores prácticas, garantía y tecnologías que se pueden utilizar para proteger la disponibilidad, integridad y confidencialidad de los activos en las infraestructuras conectadas, pertenecientes al gobierno, las organizaciones privadas y los ciudadanos; estos activos incluyen dispositivos informáticos conectados, personal, infraestructura, aplicaciones, servicios digitales, sistemas de telecomunicaciones y datos en el entorno digital.

2. Componentes de una Estrategia Nacional de Ciberseguridad

De acuerdo con la experiencia de México y de organizaciones internacionales en la materia, los siguientes son los **componentes básicos de una Estrategia Nacional de Ciberseguridad.**

2.1 Visión y objetivos claros

- **Visión general**. Es preciso generar una declaración de la visión a largo plazo que refleje el estado deseado para la ciberseguridad nacional. Esta visión será útil para la definición de indicadores.
- **Objetivos estratégicos**. Se trata de establecer un conjunto de objetivos que se pretende alcanzar en el marco de la estrategia, los cuales deben referir a temas como la protección de infraestructuras críticas, los mecanismos para la defensa contra ciberataques, la formación de capacidades en diferentes sectores y la promoción de la confianza digital[6].
- Es importante incluir en la visión la orientación a la cooperación internacional y la resiliencia ante amenazas cibernéticas.

2.2 Enfoque basado en gestión de riesgos

- **Análisis de las principales amenazas**. Esto implica entender, identificar y evaluar las ciber amenazas más significativas que enfrenta el país, incluyendo las vulnerabilidades de actores gubernamentales y privados.
- **Evaluación de riesgos**. Se debe hacer un análisis y clasificación de los riesgos asociados a estas amenazas y su impacto potencial en la seguridad nacional, la economía y la sociedad. Con base en esto, se hará la priorización de acciones para su mitigación.
- **Comunicación de riesgos.** La estrategia debe contemplar mecanismos efectivos de comunicación con los grupos interesados sobre los riesgos identificados, la estrategia para su mitigación y las lecciones aprendidas a partir de incidentes.

[6] Disponible en: Vigilancia_en_Ciberseguridad_Boletin5Confianzadigital_22-mayo_2024_ICAT.pdf (unam.mx)

- **Enfoque proactivo** para la prevención de riesgos y la evaluación continua de amenazas, así como la resiliencia.

2.3 Marco legal y normativo

- **Legislación**. La estrategia debe servir para actualizar el marco legal y este a su vez apoyarla en leyes y reglamentos que aborden integralmente la ciberseguridad, la privacidad de los datos y la protección de la información. Es importante tener presente que la legislación no debería concentrarse exclusivamente en temas de defensa y cibercrimen, pues hay que abordar todos los temas que afectan a una gran diversidad de grupos de interés.

  La creación y adecuación del marco jurídico nacional en materia de ciberseguridad debe contemplar la autorregulación por parte de los concesionarios, permisionarios, distribuidores de servicios de TIC, incluida la modificación a efecto de brindar certeza jurídica al actuar de los intermediarios de Internet, y la sociedad en general, que permita el uso y aprovechamiento de las TIC y promueva una sana convivencia en el ciberespacio. Es necesario establecer una línea base que establezca un nivel mínimo a partir del cual toda parte interesada puede evolucionar mediante dicha autorregulación. La tendencia global en la actualización para el desarrollo de mecanismos de autorregulación en la era digital es vital para el desarrollo de la digitalización y clave para la prevención de riesgos y amenazas, incluida la investigación científica y tecnológica, que son clave para fortalecer la confianza entre sociedad, sector privado e instituciones públicas. Este enfoque debe estar acompañado de un marco regulador gubernamental sólido que asegure el cumplimiento de estándares mínimos. La "autorregulación" no debe convertirse en un vacío normativo; por tanto, el Estado debe actuar como garante del cumplimiento, por lo que hay que establecer mecanismos de cumplimiento supervisados por el Estado, asegurando que la autorregulación no debilite la implementación efectiva de medidas de seguridad.

  Asimismo, es importante que este enfoque de cumplimiento regulatorio sea flexible y adaptable.

- **Normas y estándares.** La ejecución del marco legal se facilita mediante normas y estándares técnicos basados en marcos de certificación y buenas prácticas (obligatorias y voluntarias) que darán la pauta a seguir para que los diferentes grupos de interés emprendan acciones reconocidas y efectivas para garantizar la seguridad de sus sistemas de información y comunicación.

  Para generar confianza entre las organizaciones y autoridades reguladoras, es necesario contar con normas internacionales, documentos de mejores prácticas[7] y evaluaciones de conformidad que no generen cargas económicas en los servicios o productos. La constatación debe basarse en hechos que deben ser medibles, repetibles y verificables, mientras que la verificación debe basarse en normas comunes que son la base de un modelo eficaz para generar confianza en la era digital. De acuerdo con los tratados internacionales en los que se establece que los miembros utilizarán

[7] Strategic Cybersecurity Talent Framework. The World Economic Forum (2024). https://www.weforum.org/publications/strategic-cybersecurity-talent-framework/

las normas internacionales pertinentes, que servirán como base para reglamentos técnicos y procedimientos de evaluación de la conformidad.[8]

- **Protección de infraestructuras críticas.** Considera las acciones encaminadas a establecer los controles y mecanismos necesarios para reducir la probabilidad de riesgos y vulnerabilidades inherentes en el uso de las TIC para la gestión de infraestructuras críticas, así como para fortalecer la capacidad de resiliencia para mantener la estabilidad y continuidad de los servicios en caso de sufrir un incidente de ciberseguridad. En este dominio, se debe adoptar un enfoque de responsabilidad compartida que puede ser medida y evaluada con referencia a estándares internacionales.

- **Identificación de infraestructuras críticas**. La estrategia debe darle un lugar prioritario a la definición y clasificación de las infraestructuras esenciales que requieren medidas especiales de protección por el impacto potencial que podría tener en caso de que fueran objeto de ciberataques.

- **Medidas de protección**. Se debe identificar un conjunto de hojas de ruta para el desarrollo e implementación de medidas de seguridad específicas para proteger estas infraestructuras críticas en caso de ciberataques.

- **Gobernanza**. Los procesos mencionados deben diseñarse y ejecutarse de forma rápida y coordinada entre los diferentes grupos e instituciones interesadas (*stakeholders*). Para este efecto, es necesario construir mecanismos de análisis, consulta y decisión propios de los sistemas de gobernanza. Los mecanismos de comunicación y mejora continua deben incluir el diálogo constante con organizaciones de disciplinas que tienen relación e incidencia sobre la ciberseguridad (por ejemplo, inteligencia artificial y tecnologías cuánticas)[9].

- **Derechos humanos y ética**. Se deben considerar los derechos humanos y principios éticos en la estrategia, para asegurar que las políticas de ciberseguridad respeten a los primeros. Esto es importante porque la ciberseguridad debe alinearse con los estándares internacionales en materia de derechos humanos.

2.4 Capacitación y concientización en materia de ciberseguridad

El desarrollo de recursos humanos expertos en ciberseguridad, que cuenten con conocimientos especializados, requiere de planes y estrategias de capacitación y formación de especialistas a nivel nacional. El Estado puede considerar acciones para desarrollar la capacidad de expertos con carreras y postgrados, incorporar los conceptos de ciberseguridad en las escuelas en todos los niveles y promover la profesión de ciberseguridad con el marco laboral.

A nivel mundial, la formación de especialistas a nivel técnico, licenciatura y posgrado presenta un déficit en constante crecimiento: cada año, son más los puestos disponibles que el número de

---

[8] Disponible en: https://www.wto.org/english/tratop_e/tbt_e/tbt_e.htm

[9] Transition to a Quantum-Secure Economy. The World Economic Forum (2022). https://www.weforum.org/publications/transitioning-to-a-quantum-secure-economy/
Quantum Readiness Toolkit: Building a Quantum-Secure Economy. The World Economic Forum (2023). https://www.weforum.org/publications/quantum-readiness-toolkit-building-a-quantum- secure-economy/

egresados y profesionales disponibles en el mercado. Esta realidad requiere ser abordada y resuelta mediante una estrategia que incluya incrementar el número de programas universitarios, así como el reentrenamiento de profesionales que deseen integrarse al mercado de la ciberseguridad, mediante programas de capacitación impartidos en plazos cortos.

Como un componente crucial de la prevención de la ciberdelincuencia y del desarrollo de la madurez cibernética, la concientización de los diversos grupos de interés es esencial. El enfoque a ser adoptado es diferente de acuerdo con los niveles de desarrollo nacional. Se deben incorporar esfuerzos en la estrategia nacional y en campañas del gobierno y sector privado sobre la seguridad de la red, la educación y difusión sobre ciberseguridad. También se deben considerar políticas de ciberseguridad, planes de acción y medición de la madurez digital.

- **Educación y formación**. El tema de ciberseguridad requiere de recursos humanos calificados y ciudadanos conscientes de los riesgos y su respuesta a incidentes. Por ello, la estrategia debe contemplar programas de capacitación para profesionales de ciberseguridad y campañas de concientización pública para aumentar el conocimiento y ofrecer al ciudadano una guía de acciones ante las ciber amenazas.

  Es esencial no solo formar expertos en ciberseguridad, sino fomentar ambientes con conciencia digital mediante la alfabetización en todos los niveles de la población involucrados en el fenómeno tecnológico. Para ello se requiere diseñar e implementar programas educativos centrados tanto en las habilidades básicas para el manejo de las tecnologías de la información y de la comunicación como en las prácticas cotidianas para el uso seguro de las tecnologías. Esto solo puede ser logrado mediante un entendimiento de la realidad tecnológica de las comunidades de interés que puede ser llevado a cabo mediante encuestas de alfabetización digital y estudios en los que participen reguladores, el sector privado y los implementadores de política pública.

- **Desarrollo de capacidades**. Para generar una base de personal calificado en competencias de ciberseguridad, se requiere emprender iniciativas para fortalecer las capacidades técnicas y operativas de las instituciones públicas y privadas en ciberseguridad. Esto implica la realización de acuerdos y programas público-privados para potenciar las directrices de acción. Dado el déficit mundial y nacional en expertos mencionado en párrafos anteriores, es prioritario diseñar e implementar un portafolio educativo amplio, que incluya la formación de nuevos especialistas, así como el reentrenamiento de ingenieros y científicos mediante cursos cortos y/o programas de formación corporativa.

2.5 Cooperación interinstitucional e internacional

Se deben desarrollar estrategias de colaboración multidisciplinaria de las diferentes partes (actores y sectores), con un enfoque de gobernanza de Internet en materia de ciberseguridad, que permita el desarrollo integral, transversal y holístico de la Estrategia y facilite la participación abierta y transparente de los mismos.

- **Colaboración internacional**. Dado que la ciberseguridad es un problema global con situaciones transfronterizas, es fundamental contemplar la gestión de mecanismos de cooperación con otros países y organizaciones internacionales para abordar amenazas cibernéticas globales.

- **Asociaciones público-privadas**. De igual forma, la promoción de alianzas para la colaboración entre el gobierno y los sectores privado y académico es fundamental para compartir información y recursos en la lucha contra las ciber amenazas, así como con actores clave a nivel internacional con el fin de crear planes de acción conjuntos.

2.6 Respuesta y recuperación.

- **Planes de respuesta a incidentes**. Es necesario planificar el desarrollo de procedimientos y equipos especializados para coordinar y responder rápidamente a incidentes de ciberseguridad que ocurran en diferentes sectores.

- **Recuperación y resiliencia**. Es esencial que se contemplen diversas estrategias para asegurar la continuidad de las operaciones de entidades públicas y privadas, y los mecanismos para la recuperación rápida de los sistemas después de un ciberataque.

2.7 Innovación y desarrollo tecnológico

Un objetivo fundamental y parte de la naturaleza de la ciberseguridad son los avances tecnológicos y la proliferación de innovaciones digitales intrínsecas al funcionamiento de las sociedades, las empresas y los gobiernos. El potencial de crecimiento nacional impulsado por el desarrollo digital es muy relevante y la ciberseguridad no debe constituir un obstáculo en el camino sino un puente hacia el crecimiento. Por ello, las medidas de seguridad excesivamente estrictas pueden llevar al país a perder las oportunidades de innovación y progreso. Se debe evitar la tentación en la legislación de generar cargas excesivas a los actores y organizaciones, derivadas de controles extremos, porque pueden reducir su capacidad de crecimiento. El objetivo de la Estrategia Nacional de Ciberseguridad (en adelante "la Estrategia") debe ser fomentar el progreso con base en transacciones digitales seguras, no la obstaculización por regulación restrictiva y/o excesiva.

Por ello, es esencial que se generen tecnologías y soluciones de ciberseguridad que sean sencillas, económicas y eficaces, lo cual demanda la realización de actividades de investigación y desarrollo en ciberseguridad.

El diseño de una legislación en materia de ciberseguridad debe encontrar el equilibrio entre seguridad y desarrollo. El equilibrio adecuado creará un entorno digital seguro que estimularía el desarrollo sostenible de las TIC, y este desarrollo permitiría el crecimiento de la economía digital nacional y el bienestar social. El Estado puede así lograr el compromiso y colaboración de las partes interesadas con una visión compartida y unificada del desarrollo seguro.

- **Investigación y desarrollo**. Dado que los ciberataques y las tecnologías que emplean están en continua evolución, la Estrategia requiere la promoción y ejecución oportuna de programas y proyectos de investigación, así como el desarrollo de nuevas tecnologías de ciberseguridad.

- **Adopción de tecnología**. De igual manera, es necesario fomentar la adopción de tecnologías avanzadas y prácticas innovadoras para mejorar la ciberseguridad en el ámbito de los diferentes grupos de interés.

En diversos casos, la actualización de tecnologías resultará de combinar los dos enfoques mencionados. Por ejemplo, el desarrollo e implementación de protocolos de criptografía capaces

de resistir ataques de computadoras cuánticas, requiere tanto de investigación y desarrollo nacional como del trabajo colaborativo y adopción de ciertos componentes tecnológicos desarrollados en otras partes del mundo[10].

2.8 Inversión

- **Presupuesto gubernamental**. La Estrategia debe contemplar un plan de inversiones gubernamentales para sustentar los programas y acciones a su cargo.
- **Incentivos a la inversión privada en ciberseguridad**. A fin de propiciar que las empresas adopten soluciones y capaciten a su personal, es importante que existan incentivos tributarios y apoyos directos, principalmente para empresas pequeñas.
- Incluir estrategias de financiamiento a largo plazo y alianzas con el sector privado para proyectos de innovación.

3. Ciclo de vida de una Estrategia Nacional de Ciberseguridad

A fin de entender los pasos que México debe realizar para desarrollar una Estrategia Nacional de Ciberseguridad y los posibles mecanismos para su implementación, se recomienda que el ciclo de vida de dicha estrategia sea segmentado en cinco fases:

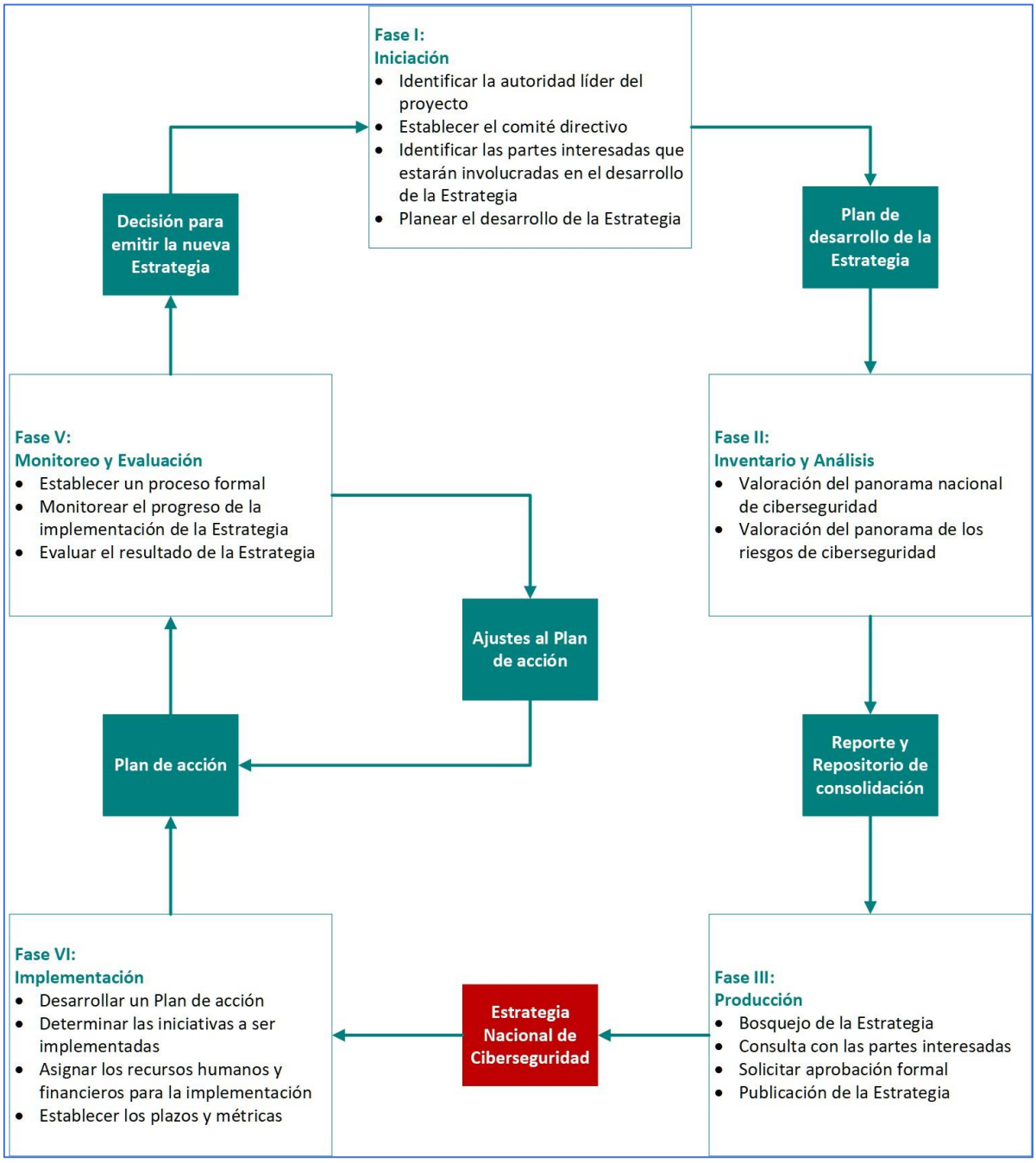
- Fase I. Iniciación.
- Fase II. Inventario y análisis.
- Fase III. Producción.
- Fase IV. Implementación.
- Fase V. Monitoreo y evaluación.

Es importante mencionar que, en todo el ciclo de vida de la Estrategia deben considerarse las condiciones, necesidades y requerimientos específicos definidos por nuestro país, así como la integración de los principios generales y las buenas prácticas que se abordarán en los numerales 3 y 4.

En la Figura 1 se muestra un resumen del ciclo de vida de una Estrategia Nacional de Ciberseguridad.

[10] Post-Quantum Cryptography. National Institute of Standards and Technology (2024). https://www.nist.gov/pqcrypto

Figura 1. Ciclo de vida de una Estrategia Nacional de Ciberseguridad



Tomado de: Guía para la Elaboración de una Estrategia Nacional de Ciberseguridad. UIT.

3.1 Iniciación y diagnóstico

Esta fase tiene el objetivo de proporcionar las bases para el desarrollo planificado y eficiente de la Estrategia, centrándose en sus componentes fundamentales, los procesos asociados, los plazos y la

identificación de las partes interesadas clave que deben participar en su elaboración. En esta fase se elaborará un plan para el desarrollo de la Estrategia.

El plan requerirá la aprobación del Ejecutivo, lo cual implica su presentación, de acuerdo con los requisitos establecidos para someter una propuesta de esta naturaleza.

3.1.1 Identificar a la Autoridad Líder del Proyecto

El Poder Ejecutivo debe designar una entidad pública (preexistente o de nueva creación), para que lidere el diseño, desarrollo y coordinación de la Estrategia. Esta entidad será referida como la Autoridad Líder del Proyecto, la cual debe ser neutral durante todo el proceso de desarrollo. Con este fin, se recomienda que esta entidad sea diferente de las organizaciones que se encargarán de la aplicación de la Estrategia, o que se adopten mecanismos para evitar la competencia entre entidades del gobierno por los recursos para la ejecución de la Estrategia.

3.1.2 Establecer el Comité Directivo

También es fundamental para la adecuada gobernanza establecer un Comité Directivo para trabajar con la Autoridad Líder del Proyecto en el desarrollo de la Estrategia. Este Comité debe estar facultado para proporcionar orientación, así como para evaluar el progreso de la Estrategia y asegurar la calidad, garantizar la transparencia y la inclusividad del proceso.

3.1.3 Identificar las partes interesadas que estarán involucradas en el desarrollo de la Estrategia

La Autoridad Líder del Proyecto debe identificar a todas las partes interesadas, tanto del sector público como de la iniciativa privada y la academia, que participarán en el desarrollo de la Estrategia. También se deben definir las funciones de las diferentes partes interesadas y describir cómo colaborarán para gestionar las actividades y atender las diversas expectativas a lo largo del proceso. Para incluir la representación de todos los sectores de la sociedad que se verán afectados por el proyecto estratégico, la Autoridad podría contar con un Consejo Asesor, avalado por el Comité Directivo, que pueda brindar conocimiento experto para la mejor toma de decisiones en todas las fases del ciclo de vida de la Estrategia.

El ciclo de vida de la Estrategia debe contemplar enfoques de todas las partes interesadas que incluyan a la sociedad civil, la comunidad técnica, científica, operadores de servicios de telecomunicaciones, empresas y cámaras sectoriales. Estos actores contribuirán a la identificación y puesta en marcha de soluciones para mitigar los riesgos, aportando perspectivas desde cada sector al Comité. El sector privado se posicionará como un proveedor de información fundamental acerca de las ciber amenazas a las que se enfrentan las empresas, mientras que la academia aportará conocimiento relacionado con las técnicas y mecanismos más recientes, así como colaborar con la industria y reguladores en el diseño y puesta en marcha de pruebas de estrés y de cumplimiento de la normatividad vigente, incluyendo desarrollos tecnológicos recientes y tendencias en la investigación, agregando conocimiento, análisis, discusiones en foros internacionales, así como sobre posibilidades de colaboración en el desarrollo de futuros talentos. Asimismo, las organizaciones de la sociedad civil podrían analizar las implicaciones de las políticas de seguridad en temas torales como los derechos humanos, evaluando el impacto de las políticas en los diferentes

miembros de la sociedad, principalmente en relación con las garantías a su privacidad y uso de datos personales. Dentro del sector público, las secretarías, organismos judiciales, organismos encargados de hacer cumplir la ley y las autoridades nacionales de defensa pueden aportar su visión de los riesgos y amenazas desde la perspectiva de la gestión gubernamental.

3.1.4 Identificar los recursos humanos y financieros

La Autoridad Líder del Proyecto debe determinar los recursos humanos y financieros necesarios para diseñar y aplicar la Estrategia, y de dónde podrían obtenerse. Es fundamental la financiación a largo plazo para todo el ciclo de vida de la Estrategia, incluidos su desarrollo, aplicación y perfeccionamiento.

3.1.5 Planear el Desarrollo y Ejecución de la Estrategia

La Autoridad Líder del Proyecto debe preparar un plan para desarrollar la Estrategia, que deberá ser presentado al Comité Directivo y al Poder Ejecutivo, para su aprobación.

El plan de desarrollo de la Estrategia debe identificar los principales pasos y actividades, las partes interesadas clave, los plazos y los recursos requeridos, incluidos los humanos y financieros. Debe especificar cómo y cuándo se espera que las partes interesadas pertinentes participen en el proceso de desarrollo para brindar aportaciones y comentarios. Además, debe considerar si la Estrategia adoptará la forma de legislación o política.

3.2 Inventario y análisis

El Consejo Asesor recopilará datos sobre ciberseguridad y la tipología de riesgos actuales y futuros, con el objetivo de crear un informe que resuma la postura estratégica nacional en este ámbito, para presentarlo al Comité Directivo. La Autoridad Líder del Proyecto analizará la información para identificar áreas de oportunidades o potenciales amenazas a la capacidad de ciberseguridad y propondrá opciones para abordarlas. Como consecuencia del análisis, se debe realizar una evaluación de los entornos normativos y operativos existentes, a la par de los resultados deseados para la estrategia y los medios disponibles para alcanzar los objetivos.

3.2.1 Valoración del panorama de ciberseguridad nacional

Se debe realizar un análisis de las fortalezas y debilidades del país en materia de ciberseguridad. La Autoridad Líder del Proyecto, con el apoyo del Consejo Asesor, debe hacer un balance de las funciones y responsabilidades de las diferentes partes interesadas en materia de ciberseguridad, así como identificar los activos y servicios críticos para el buen funcionamiento de la sociedad y la economía (infraestructura crítica), y mapear las leyes, regulaciones, políticas, programas y capacidades nacionales existentes en lo que se refiere a la seguridad cibernética. El análisis se someterá a la consideración del Comité Directivo para que se tome como base para la toma de decisiones posterior.

Es importante resaltar la importancia que tiene el estudio de los distintos grupos demográficos incluidos en una estrategia de esta naturaleza. Por ello resulta necesario generar instrumentos que permitan evaluar el estado tecnológico de las comunidades para identificar brechas de conocimiento y habilidades, así como de disponibilidad tecnológica y formas de interacción con las

plataformas digitales. Así, la Estrategia toma en cuenta la realidad de las comunidades y responde ante las necesidades de las personas.

3.2.2 Revisión Integral y Actualización de Legislación

La Estrategia debe contemplar una revisión integral del marco normativo existente, con un enfoque hacia la armonización con normativas internacionales como el Convenio de Cibercriminalidad de la Organización de las Naciones Unidas (ONU). Esto garantizaría una cobertura amplia que considere no sólo los aspectos de defensa y cibercrimen, sino también privacidad de datos, propiedad intelectual, y protección de derechos fundamentales en el entorno digital.

3.2.3 Valoración del panorama de riesgos de ciberseguridad

La Autoridad Líder del Proyecto debe evaluar los riesgos a los que se enfrentan la nación y los diversos grupos de interés relacionados con la ciberseguridad, mediante la identificación de los activos digitales nacionales, tanto públicos como privados, sus interdependencias, vulnerabilidades y amenazas, y una estimación de la probabilidad y el impacto potencial de los incidentes cibernéticos. Lo anterior bajo un esquema de Gestión de Riesgos que permita llevar a cabo un análisis cuantitativo de los riesgos potenciales.

3.3 Producción: elaboración de la Estrategia

El propósito de esta fase es desarrollar el texto de la Estrategia mediante la participación de las principales partes interesadas del sector público, el sector privado y la sociedad civil a través de una serie de consultas públicas y la organización de grupos de trabajo para elaborar las diferentes secciones, bajo la coordinación de la Autoridad Líder del Proyecto y el apoyo del Consejo Asesor.

La Autoridad Líder del Proyecto, junto con el Comité Directivo, debe avalar la redacción de la Estrategia. El documento final debe proporcionar la dirección para el país, expresar una visión, objetivos y alcance claros, con plazos específicos, y priorización de programas y acciones en función de su impacto en la sociedad, la economía y la infraestructura crítica. Además, la estrategia debe identificar posibles acciones, fomentar la implementación y asegurar la asignación de recursos necesarios. Puede incorporar conclusiones de la fase de Inventario y Análisis. También, debe designar la entidad responsable de la gestión y evaluación de la Estrategia, así como una entidad encargada de su aplicación general, que funja como una autoridad central o comisión nacional de ciberseguridad.

3.3.1 Consulta dirigida a una amplia gama de partes interesadas nacionales, regionales e internacionales

El proyecto final de la Estrategia debe difundirse entre un amplio grupo de partes interesadas, no limitado a los que participaron en los procesos de desarrollo de la estrategia. Se esperaría que los comentarios y opiniones sean utilizados para finalizar la Estrategia.

Solicitud de aprobación formal

La Autoridad Líder del Proyecto debe asegurarse de que el Ejecutivo apruebe el proyecto final y adopte formalmente la Estrategia. Este proceso oficial de adopción variará según los tiempos y procedimientos normativos establecidos y considerará la forma en que, eventualmente, se conozca

en el marco del poder legislativo, a fin de preparar su posible actuación en la emisión de las leyes respectivas.

Publicación y promoción de la Estrategia

La Estrategia debe convertirse en un documento público, con amplia difusión, y debe estar fácilmente disponible. Lo ideal es que la puesta en marcha de la Estrategia vaya acompañada de actividades de divulgación en los sectores público, privado y académico.

Implementación

La fase de implementación es el elemento más importante del ciclo de vida de la Estrategia, pues se centra en seguir la guía del Plan de Acción, ejecutando los programas y acciones contemplados.

Desarrollo del Plan de Acción

Las partes interesadas, incluyendo gobierno, sociedad civil, academia y sector privado, deben participar y coordinarse, para desarrollar el plan de acción asociado a la Estrategia. La Autoridad Líder del Proyecto debe proporcionar un mecanismo expedito y eficaz para reunir a las partes interesadas con el fin de acordar objetivos y resultados de cada programa, así como los mecanismos para coordinar esfuerzos y reunir recursos.

Determinar las iniciativas a implementar

En el Plan de Acción, la Autoridad Líder del Proyecto debe identificar las iniciativas específicas dentro de cada área prioritaria de la Estrategia, las cuales serán los instrumentos prácticos para alcanzar los objetivos de la Estrategia. El cronograma, recursos y esfuerzos necesarios para la implementación de estas iniciativas deben priorizarse de acuerdo con su importancia para garantizar que los recursos se aprovechen adecuadamente.

Asignación de los recursos humanos y financieros para la implementación

Después de identificar las iniciativas prioritarias, la Autoridad Líder del Proyecto debe designar entidades gubernamentales específicas como propietarias de cada iniciativa. Estas entidades serán responsables de ejecutar las iniciativas asignadas, coordinando con otras partes interesadas. Para asegurar el éxito, la Autoridad Líder del Proyecto evaluará si estas entidades tienen el mandato y los recursos necesarios, y colaborará con ellas para hacer los arreglos pertinentes para gestionar todo tipo de recursos requeridos, incluyendo personal, infraestructura, tecnología y financiamiento.

Establecimiento de plazos y métricas

El último componente crucial del Plan de Acción es la creación de métricas e indicadores clave de desempeño (KPI) para evaluar cada iniciativa, como las que involucran campañas de concienciación o las relacionadas con la ejecución de ejercicios de ciberseguridad. La métrica debe definirse en función de criterios objetivos. La Autoridad Líder del Proyecto, en colaboración con el Consejo Asesor y los operadores pertinentes de cada iniciativa, debe desarrollar estos indicadores y establecer plazos específicos para su implementación. Se debe motivar a los operadores a definir y mantener parámetros medibles y detallados para facilitar la evaluación continua de la eficiencia y eficacia de las iniciativas.

Monitoreo y evaluación

El desarrollo e implementación de la estrategia son procesos continuos que requieren supervisión y evaluación. En la fase de monitoreo se debe establecer un proceso formal, liderado por la Autoridad Líder del Proyecto, para supervisar la implementación de la Estrategia según su Plan de Acción y las diferentes iniciativas derivadas de dicho plan. En la fase de evaluación, el Ejecutivo, la Autoridad Líder del Proyecto y el Comité Directivo deben revisar la pertinencia continua de la estrategia frente al cambiante panorama de riesgos, asegurándose de que aún refleje los objetivos gubernamentales y realizando ajustes según sea necesario.

El seguimiento requiere también poner el énfasis en los cambios que la estrategia tiene en los diversos grupos demográficos. Para medir sus efectos resulta necesario el diseño de instrumentos de análisis como son las encuestas de alfabetización digital, evaluaciones de conocimientos y estudios sobre el despliegue tecnológico, sus riesgos y las problemáticas detectadas por las poblaciones.

Establecimiento de un procedimiento formal

Para asegurar que la implementación de la Estrategia sea monitoreada y evaluada efectivamente, el Comité Directivo debe designar una entidad independiente responsable para supervisar y evaluar los progresos y la eficiencia de la implementación. Esta entidad colaborará en la definición de parámetros de monitoreo y evaluación, que deben establecerse de acuerdo con la metodología SMART (*Specific, Measureable, Achievable, Realistic, Time-bound*, por sus siglas en inglés) para facilitar el seguimiento y resaltar las áreas de mejora.

Monitoreo del progreso de la implementación de la Estrategia

La entidad encargada de supervisar la implementación de la Estrategia debe seguir un calendario acordado a lo largo de todo el ciclo de vida de la Estrategia para hacer evaluaciones de avance. Como resultado de la supervisión, se deben señalar las posibles desviaciones del cronograma acordado, identificando las causas de los retrasos y las medidas para corregirlos. Las partes interesadas deben presentar informes por los compromisos establecidos, permitiendo identificar problemas de implementación rápidamente. Esto facilitará que el gobierno corrija la situación o ajuste sus planes, basándose en lecciones aprendidas durante la implementación.

Respuesta y recuperación

- **Planificación de respuestas a incidentes:** Establecer procedimientos claros para la respuesta y recuperación ante incidentes de ciberseguridad.
- **Gestión de crisis y resiliencia:** Implementar mecanismos para asegurar la continuidad de los servicios esenciales en caso de un ciberataque, incluyendo la recuperación rápida.

Evaluación de los resultados de la Estrategia

Es esencial que el progreso en las métricas acordadas sea evaluado regularmente, es decir, comparar los resultados obtenidos con los objetivos de la Estrategia, a fin de determinar si las iniciativas están alineadas y se están cumpliendo los objetivos o si se necesitan acciones diferentes. Esta información debe ser entregada a la Autoridad Líder del Proyecto, junto con propuestas para actualizar el Plan de Acción, el cual debe permitir ajustes de acuerdo con los cambios que surjan en el entorno normativo y el panorama de riesgos. Los resultados de la evaluación permitirán la revisión

general de la Estrategia por el Comité Directivo, considerando el progreso y los cambios externos, así como una reevaluación de las prioridades y objetivos del Ejecutivo.

También se debe considerar el objetivo de comprender mejor el grado de compromiso de México en materia de ciberseguridad, identificar los posibles rezagos, fomentar la adopción de buenas prácticas y proporcionar información útil para que el país mejore sus posturas y desempeño en materia de ciberseguridad. Las métricas y resultados para medir la mejora y un fortalecimiento general se componen de cinco pilares donde se destacan las prácticas del país:

- Medidas jurídicas. Medición de las leyes y reglamentos sobre ciberdelincuencia y ciberseguridad;
- Medidas técnicas. Medición de la aplicación de las capacidades técnicas e incentivos para su manejo, a través de los organismos nacionales y sectoriales;
- Medidas institucionales. Medición de las estrategias nacionales y organizaciones que aplican la ciberseguridad;
- Medidas de capacitación. Medición de las campañas de sensibilización, formación, educación e incentivos para la capacitación en materia de ciberseguridad, y
- Medidas de cooperación. Medición de asociaciones entre organismos, empresas y entre países.

Actualización y renovación

- **Revisión periódica:** actualizar la Estrategia en función de los cambios tecnológicos, nuevas amenazas y lecciones aprendidas.
- **Innovación continua:** incluir la investigación y el desarrollo de nuevas tecnologías de ciberseguridad que mantengan la estrategia a la vanguardia.

4. Principios generales

Hay diez principios transversales que deben ser considerados en todas las fases del desarrollo de la Estrategia.

4.1 Visión

Una estrategia tiene más probabilidades de éxito cuando establece una visión clara que ayuda a todas las partes a comprender la importancia y necesidad de la estrategia (contexto), lo que se debe lograr (objetivos) y a quién impactará (alcance). Por lo tanto, la Estrategia debe definir una visión clara del gobierno y la sociedad, asegurándose de que los objetivos y el calendario de implementación estén alineados con esta visión.

4.2 Enfoque integral y prioridades adecuadas

Es esencial comprender la ciberseguridad con todos sus aspectos y la forma en que estos interactúan, ya que pueden complementarse o competir entre sí. Estos aspectos abarcan lo técnico, económico, social, legal, seguridad nacional e internacional, relaciones internacionales, negociaciones comerciales y desarrollo sostenible. Al comprender estos elementos y analizar el contexto específico del país, se pueden establecer prioridades alineadas con los objetivos y el calendario de ejecución de la Estrategia. El enfoque integral también implica abarcar a los diferentes grupos de interés y no concentrarse sólo en actores gubernamentales.

4.3 Inclusividad

La Estrategia debe ser desarrollada con la participación de todas las partes interesadas relevantes, abordando sus necesidades y responsabilidades. El gobierno, el sector privado y la sociedad civil deben colaborar en las negociaciones y en la implementación de la Estrategia. El incluir una perspectiva de género en una estrategia nacional de ciberseguridad es esencial no sólo para garantizar la inclusión, sino también para aprovechar el talento y las perspectivas diversas que pueden enriquecer la seguridad y la resiliencia en el entorno digital. Entre las razones para incluir la perspectiva de género en las estrategias nacionales de ciberseguridad, se destacan:

- Inclusión y equidad: asegurar que las políticas y estrategias incluyan a todas las personas, independientemente de su género, contribuye a una sociedad más equitativa.
- Diversidad en la toma de decisiones: la participación de mujeres en roles de liderazgo en ciberseguridad puede llevar a soluciones más innovadoras y efectivas, ya que aporta perspectivas diversas a los desafíos de ciberseguridad.
- Cierre de la brecha digital de género: al abordar la brecha digital de género, se puede aumentar la participación de mujeres en la fuerza laboral de ciberseguridad, lo que es vital para satisfacer la creciente demanda de especialistas en este campo.

4.4 Neutralidad Tecnológica

Como un principio fundamental del desarrollo digital y de la industria en el mundo. Este principio considera que ninguna tecnología, organización privada o pública, así como ningún producto, independiente del país de origen, será favorecido o perjudicado, siendo los operadores, las empresas, el sector público relevantes o los usuarios finales libres de elegir aquella tecnología que cumpla con estándares internacionales que mejor se adecúe a sus necesidades. Se debe considerar que cualquier política pública tenga la suficiente flexibilidad y capacidad de adaptarse a los cambios tecnológicos que cada vez se van produciendo de manera más rápida y vertiginosa.

4.5 Prosperidad económica y social

Es importante mencionar que la ciberseguridad no es un objetivo en sí mismo; la Estrategia debe centrarse en los ciudadanos y fomentar la prosperidad económica y social, maximizando la contribución de las TIC al desarrollo sostenible y la inclusión social. Debe estar en consonancia con los objetivos socioeconómicos del país y generar la confianza necesaria para alcanzar estos objetivos y proteger al país de las ciber amenazas.

4.6 Derechos humanos fundamentales

La Estrategia debe reconocer el hecho de que los mismos derechos que las personas tienen fuera de línea también deben protegerse en línea; en consecuencia, se deben respetar los derechos humanos fundamentales y ser coherente con ellos. Por ello, es esencial prestar atención a la libertad de expresión, la privacidad de las comunicaciones y la protección de datos personales.

4.7 Gestión de riesgos y resiliencia

La Estrategia debe facilitar la gestión eficiente de los riesgos de ciberseguridad y promover la resiliencia en las actividades económicas y sociales. Aunque el entorno digital brinda oportunidades, también presenta riesgos, por lo que la Estrategia debe alentar a las entidades a priorizar sus

inversiones en ciberseguridad y gestionar proactivamente los riesgos. Dependiendo de la predisposición al riesgo de una entidad, se deben equilibrar las medidas de seguridad con los beneficios potenciales, teniendo en cuenta la naturaleza dinámica del entorno digital.

4.8 Determinar y aplicar los instrumentos de política adecuados

Los gobiernos cuentan con diferentes instrumentos de política, como legislación, reglamentación, normalización, certificaciones, incentivos, mecanismos de intercambio de información, programas educativos, intercambio de mejores prácticas, establecimiento de normas de comportamiento esperadas y creación de comunidades de confianza, entre otros. Cada instrumento tiene fortalezas y debilidades, costos y resultados diferentes. Los mejores resultados pueden lograrse seleccionando el instrumento de política más adecuado para cada objetivo, teniendo en cuenta las circunstancias específicas del país.

4.9 Liderazgo, responsabilidad compartida, roles y asignación clara de recursos

La estrategia debe establecerse en el nivel más alto del gobierno, que luego será responsable de asignar las funciones y responsabilidades pertinentes, así como suficientes recursos humanos y financieros. Una adecuada protección y promoción de la ciberseguridad requiere compartir la responsabilidad entre los distintos actores de la industria, ya sea a nivel de oferta, a nivel de usuario y a nivel de regulador. Cabe destacar que el ecosistema en esta materia es muy amplio, los cuales, si bien operan de manera individual dentro de sus respectivos ámbitos de acción, deben estar debidamente coordinados y regulados según los mismos criterios o estándares internacionales, para dar una respuesta conjunta frente a un incidente. El hecho de compartir esta responsabilidad en el actuar implica mejorar exponencialmente las condiciones al momento de producirse algún ataque. La ciberseguridad es un desafío común que enfrenta toda la sociedad, incluidos los gobiernos, los reguladores, las organizaciones de la industria, las organizaciones que generan estándares, las empresas y los proveedores de tecnologías, ya sean de hardware o software. Si la seguridad cibernética se eleva a la altura de una ideología determinada o se relaciona con factores políticos, los desafíos del ciberespacio no podrán resolverse.

4.10 Entorno de confianza

A fin de aprovechar todo el potencial de las oportunidades sociales, políticas y económicas que ofrece el uso de las TIC, la Estrategia debe construir confianza en el ecosistema digital. En tal sentido, los derechos e intereses de los usuarios deben ser protegidos, además de garantizar la seguridad de datos y sistemas. La Estrategia debe facilitar políticas y acciones para prestar servicios críticos seguros.

5. Buenas prácticas de ciberseguridad nacional

Las buenas prácticas consisten en un conjunto de elementos que permiten que la Estrategia sea exhaustiva y eficaz, al tiempo que permiten adaptarla al contexto nacional. Las naciones deben identificar y seguir las buenas prácticas que apoyen sus propios objetivos y prioridades en consonancia con la visión definida en su Estrategia. Estos elementos son agrupados en las siguientes áreas de interés:

- Gobernanza;
- Gestión de riesgos en la ciberseguridad nacional;

- Preparación y resiliencia;
- Infraestructura crítica y servicios esenciales;
- Capacitación, creación de competencias y sensibilización;
- Legislación y regulación, y
- Cooperación internacional.

5.1 Gobernanza

La gobernanza se refiere al conjunto de procesos, estructuras y mecanismos que se utilizan para tomar decisiones de forma participativa e inclusiva para implementar políticas y gestionar recursos en el marco de la Estrategia. Uno de sus objetivos es garantizar que la ciberseguridad esté integrada en el diseño organizacional, considerando a los actores de la gestión de riesgos y el marco de control interno. Este es un punto de partida para el diseño, desarrollo e implementación de una gobernanza cibernética.

5.2 Asegurar el más alto nivel de apoyo

Contar con el respaldo formal del nivel más alto de gobierno aumenta la probabilidad de que se asignen recursos suficientes y de que los esfuerzos de coordinación tengan éxito. Además, se destaca que la ciberseguridad del país está vinculada al desarrollo de la economía digital y otros aspectos sociales y políticos que constituyen una prioridad nacional, por lo que la ciberseguridad también debe estar en lo más alto de la jerarquía. Desde una perspectiva organizacional, el nivel más alto debe asumir su posición en un órgano colegiado de máximo nivel de gestión de la ciberseguridad, el cual es responsable de ratificar la estrategia de aseguramiento de la ciberseguridad. La autoridad establecida para la coordinación nacional de ciberseguridad, cumple una función muy importante como encargada de coordinar el desarrollo de la estrategia y gestionar y supervisar su implementación.

5.3 Establecer una autoridad competente en materia de ciberseguridad

La Estrategia debe establecer una autoridad nacional competente, ubicada en el nivel más alto del gobierno, encargada de ejecutar y supervisar la implementación de la Estrategia. Esta autoridad debe liderar, coordinar y reportar los progresos y resultados, junto con la definición clara de funciones, responsabilidades y procesos. La Autoridad puede requerir formalización en políticas o leyes con el objeto de asegurar su capacidad para involucrar a las partes interesadas. Asimismo, dicha autoridad puede tener el apoyo de grupos consultivos y comités interinstitucionales que apoyen los procesos de toma de decisiones en el marco de la Estrategia. El grupo consultivo debe incluir representantes del gobierno, autoridades reguladoras, de las empresas concesionarias de telecomunicaciones, plataformas digitales, proveedores de tecnología y servicios, academia, centros de investigación y profesionales expertos en la materia de ciberseguridad.

5.4 Asegurar la cooperación intragubernamental

La Estrategia debe establecer un mecanismo para identificar e incluir y vincular a las entidades gubernamentales que, por sus atribuciones, serán afectadas o responsables de su implementación. El compromiso, coordinación y cooperación entre los distintos niveles gubernamentales son

aspectos fundamentales para garantizar que los mecanismos de gobernanza y los recursos produzcan los resultados deseados de la Estrategia.

5.5 Asegurar cooperación entre sectores

La Estrategia debe reflejar una comprensión de las dependencias del sector privado y otras partes interesadas no gubernamentales nacionales para lograr un ecosistema más seguro y resiliente. Para ello, la Estrategia debe definir los procesos necesarios para que el gobierno involucre a las partes interesadas, además de definir sus roles y responsabilidades.

Los pilares de la gobernanza participativa

Participación de los diversos grupos de interés en el proceso de toma de decisiones para definir, ejecutar y evaluar la Estrategia, asegurando que se consideren diversas perspectivas y necesidades.

Transparencia para que las decisiones, acciones, avances y resultados sean accesibles para todas las partes interesadas, promoviendo la confianza y la rendición de cuentas.

Responsabilidad compartida y distribución de competencias para asegurar que las personas y entidades realicen las actividades que les corresponden y rindan cuentas por sus decisiones y comportamientos.

Eficiencia y eficacia para que los recursos destinados a la realización de la Estrategia se utilicen de manera óptima para lograr los objetivos establecidos, minimizando el desperdicio y maximizando los resultados.

Equidad para evitar la discriminación de grupos, organizaciones y tecnologías, promoviendo la inclusión, la neutralidad tecnológica y la igualdad de oportunidades.

5.6 Asignar presupuesto y recursos específicos

La Estrategia debe detallar la asignación de recursos específicos y apropiados para su implementación, mantenimiento y revisión. Los recursos deben definirse en términos de financiamiento, personas y material. La asignación de recursos no se debe considerar como un evento único, ya que las necesidades deben ser revisadas periódicamente en función de los avances o deficiencias en la ejecución de las tareas u objetivos de la Estrategia.

5.7 Desarrollar un plan de implementación

La Estrategia debe ir acompañada de un plan de implementación que detalle cómo se lograrán los objetivos, identificando la entidad responsable de cada tarea, los recursos necesarios, los procesos que se utilizarán, el análisis de riesgos de ejecución, los mecanismos de monitoreo y evaluación, y los resultados esperados.

5.8 Gestión de riesgos en la ciberseguridad nacional

Es importante mencionar que los riesgos de ciberseguridad no pueden ser eliminados en su totalidad, por lo que debe adoptarse un enfoque de gestión integral de riesgos. Si un país comprende los riesgos a los que está expuesto será capaz de manejar estos riesgos más efectivamente; por ello, la gestión de riesgos debe ser revisada periódicamente para asegurar la mejora continua.

Los pilares de la gestión integral de riesgos[11]

Identificación de riesgos mediante un proceso orientado a reconocer y analizar las amenazas y vulnerabilidades que pueden afectar a los sistemas de información.

Evaluación de riesgos para estimar el impacto potencial de las amenazas identificadas en función de la probabilidad de su ocurrencia y su severidad, y priorizar los riesgos más críticos.

Mitigación de riesgos para implementar controles y medidas de seguridad que permitan reducir sus efectos.

Monitoreo continuo para dar seguimiento constante de los riesgos y la efectividad de las medidas de seguridad implementadas.

Respuesta a incidentes orientada a preparar y ejecutar planes de acción para actuar eficaz y oportunamente ante los incidentes.

Comunicación de riesgos e intercambio de información ante incidentes de ciberseguridad como elementos esenciales para una respuesta efectiva y coordinada, así como para el aprendizaje colectivo a partir de incidentes[12].

La gestión de riesgos debe contemplar que, con el desarrollo y el uso generalizado de internet, se ha generado paralelamente una industria dedicada a buscar vulnerabilidades con el fin de cometer fraudes y ataques a las redes y sistemas informáticos. Dada la naturaleza de estas amenazas, que tienen un componente fundamentalmente técnico, la seguridad de las redes y sistemas sobre las cuales se ejecutan tales delitos es un asunto que, esencialmente, requiere preparación y capacidad de respuesta y recuperación en el ámbito técnico, que se enfrenta y se supera con soluciones técnicas también. Por lo tanto, la gestión de riesgos que no contemple la evidencia empírica no debe tener cabida ni en las políticas públicas ni en las regulaciones, ya que ello desvirtúa el sentido y la esencia de la protección a la seguridad de redes y sistemas. Una gestión de riesgos efectiva no debe mezclar intereses, ideología o criterios meramente políticos, pues no garantizan ni contribuyen a la finalidad principal que es la preservación de la ciberseguridad. La protección de los sistemas requiere una gestión de riesgos del más alto grado de profesionalismo y responsabilidad, a fin de que la postura y respuesta a las amenazas cibernéticas sea siempre realizada en forma objetiva e imparcial.

5.9 Evaluar las amenazas cibernéticas y alinear las políticas con su constante evolución y expansión

La Estrategia debe identificar las infraestructuras y los servicios críticos del país, a la par de evaluar el panorama de amenazas cibernéticas, a fin de identificar las amenazas y riesgos específicos de las infraestructuras y servicios críticos, así como a las personas que los usan y dependen de ellos. Este proceso permitirá priorizar los recursos necesarios para protegerlos.

[11] Disponible en: https://www.ibm.com/mx-es/topics/cyber-risk-management

[12] Disponible en: https://www.csirt.es/index.php/es/

5.10 Definir un enfoque de gestión de riesgos

Es necesario evaluar las amenazas cibernéticas y desarrollar un registro nacional de riesgos, que esté almacenado y sea comunicado de forma segura, además de que sea actualizado periódicamente. Esto permitirá la supervisión gubernamental de los riesgos y los enfoques adoptados para gestionarlos de forma integral y oportuna.

5.11 Identificar una metodología común para gestionar los riesgos de ciberseguridad

La Estrategia debe establecer una metodología común para la gestión de riesgos de ciberseguridad, garantizando la eficiencia y la coherencia en todas las organizaciones, además de facilitar el intercambio de información sobre amenazas y riesgos entre sistemas interdependientes. Dicha metodología guiará la asignación de roles y responsabilidades en diversos aspectos de la gestión de riesgos, como la valoración de amenazas y activos, implementación y mantenimiento de medidas mitigantes, etc. A la par, orientará la minimización de riesgos a través de una arquitectura y un diseño seguros y evaluaciones y/o auditorías periódicas.

5.12 Desarrollar perfiles sectoriales de riesgo en materia de ciberseguridad

La Estrategia, para contar con el nivel de especificidad de cada caso, requiere el uso de perfiles sectoriales de riesgo de ciberseguridad, que consisten en análisis cuantitativos de los tipos de amenazas a las que se enfrenta cada sector, para comprender el riesgo de manera más objetiva. Se desarrollarán perfiles para los sectores considerados como más críticos para la sociedad y economía del país, y se actualizarán periódicamente.

Colaborar en la actualización de bases de conocimientos para el sector de las telecomunicaciones para proporcionar orientación útil sobre la diversidad de riesgos de seguridad y medidas de mitigación del sector. Esta línea de acción, contribuye a los objetivos de poner a disposición el conocimiento combinado del ecosistema para aumentar la confianza en las redes de telecomunicaciones y construir un entorno digital interconectado más seguro. Esta estrategia, proporciona información esencial para el desarrollo de perfiles, así como orientación y recomendaciones de las mejores prácticas y medidas de mitigación de riesgos.

5.13 Establecer políticas de ciberseguridad

La Estrategia debe fomentar el establecimiento de políticas de ciberseguridad para las entidades nacionales críticas, como las autoridades gubernamentales y los operadores de infraestructuras críticas, entre otras. Dichas políticas deben abarcar los requisitos de gobernanza, operativos y técnicos, e instruir a las partes interesadas sobre sus funciones y responsabilidades, así como orientar u ordenar enfoques específicos sobre estas cuestiones.

5.14 Preparación y resiliencia

Esta área de interés busca apoyar el establecimiento y la sostenibilidad de capacidades nacionales para prepararse, prevenir, detectar, mitigar y responder oportuna y eficazmente a incidentes graves de ciberseguridad, para mejorar la ciber resiliencia del país y las diversas organizaciones que pudieran ser afectadas.

La ciber resiliencia es la capacidad de una organización para anticiparse, resistir, recuperarse y adaptarse a incidentes cibernéticos que pueden causar daños o pérdidas. Este concepto debe ir más

allá de la mera prevención, centrándose en la habilidad de responder y recuperarse de ataques o interrupciones, pues implica tener medidas de seguridad robustas, planes de respuesta a incidentes bien definidos y la capacidad de restaurar rápidamente las operaciones normales después de un ataque, así como la elaboración de protocolos para prevenir futuros incidentes[13].

5.15 Establecer entidades de respuesta ante incidentes de ciberseguridad

La Estrategia debe incluir el establecimiento de entidades nacionales encargadas de responder a incidentes, las cuales deben tomar acciones proactivas y reactivas, así como proporcionar servicios preventivos y educativos. Estas entidades contribuirán a fortalecer la capacidad de respuesta y recuperación de un país frente a ciberataques, así como mejorar su resiliencia ante las ciber amenazas.

5.16 Establecer planes de contingencia para la gestión de crisis de ciberseguridad y recuperación de desastres

La Estrategia debe involucrar un plan nacional de contingencia para emergencias y crisis de ciberseguridad, integrado en el plan nacional de contingencia general del país, o alineado con él. Debe manejarse un plan específico para las Infraestructuras Críticas de Información (ICI). El plan de contingencia debe considerar los hallazgos de las evaluaciones nacionales de riesgos que puedan afectar las operaciones de las Infraestructuras Críticas (IC) e ICI, así como a los mecanismos de recuperación en caso de catástrofe. Además, debe proporcionar una visión general de los mecanismos nacionales de respuesta a incidentes, junto con la clasificación y escalamiento de los incidentes según su impacto en los activos y servicios críticos.

5.17 Promover la compartición de información

La Estrategia debe establecer mecanismos que permitan el intercambio de información sobre amenazas entre los sectores público y privado. Para esto, debe identificarse una o más autoridades responsables de transmitir información precisa y procesable entre la comunidad nacional de ciberseguridad, incluidos los sectores público y privado. También debe contemplarse una serie de mecanismos de sensibilización de organizaciones públicas y privadas para que participen en el intercambio de información sobre riesgos e incidentes.

5.18 Realizar ejercicios de ciberseguridad

La Estrategia debe promover la organización y coordinación de ejercicios nacionales e internacionales de ciberseguridad y respuesta a incidentes. Estos ejercicios ayudarán a desarrollar la capacidad de respuesta efectiva a incidentes, poner a prueba los procedimientos de gestión de crisis y los mecanismos de comunicación, y verificar la capacidad operativa de las entidades de respuesta ante incidentes de ciberseguridad.

5.19 Establecer la evaluación de impacto o gravedad de los incidentes de ciberseguridad

La Estrategia debe fomentar la evaluación de la gravedad de los incidentes de ciberseguridad en función de su impacto en activos, servicios e infraestructuras críticos, así como en las personas. Esto, con el fin de entender el contexto general del incidente, analizando sus impactos potenciales y

[13] Disponible en: https://www.ibm.com/es-es/topics/cyber-resilience.

reales en diferentes sectores y/o grupos de población, junto con sus efectos en cascada. Estas evaluaciones deben realizarse siguiendo un método validado, en consulta con una amplia gama de partes interesadas de manera abierta, inclusiva y transparente, y deben integrarse al plan nacional de contingencia y recuperación frente a un ataque de seguridad.

5.20 Infraestructura y servicios críticos

La Estrategia debe promover la seguridad y la continuidad de las IC y las ICI, dado que las consecuencias de un incidente que las afecte pueden perturbar el orden social, la prestación de servicios esenciales y el bienestar económico de un país.

Se identifica a las IC como activos esenciales para el funcionamiento y la seguridad de la sociedad y a economía. Por su parte, las ICI se definen como sistemas informáticos y las TIC que operan funciones clave de la infraestructura crítica de una nación o sector.

5.21 Establecer un enfoque de gestión de riesgos para identificar y proteger las infraestructuras críticas y los servicios esenciales

La Estrategia debe reconocer la importancia de proteger a las IC y las ICI contras riesgos cibernéticos y diseñar un enfoque integral de gestión de riesgos. Se debe realizar una evaluación detallada de los riesgos orientada a la identificación de las IC e ICI nacionales y de los servicios esenciales, cuya perturbación pueda tener un impacto grave en la salud, la seguridad o el bienestar económico de los ciudadanos, o en el funcionamiento eficaz de la administración pública o la economía. La Estrategia debe incluir una lista específica de IC y/o ICI y su correlación, que puede revisarse y actualizarse periódicamente según sea necesario.

5.22 Adoptar un modelo de gobernanza para la protección de Infraestructuras Criticas

Este modelo de gobernanza debe contemplar responsabilidades claras, en los escenarios tanto de IC e ICI. La Estrategia debe detallar la estructura de gobernanza, las funciones y las responsabilidades de las diferentes partes interesadas en la protección de las IC y las ICI. El modelo debe incluir la identificación de las entidades gubernamentales encargadas de verticales específicas, las responsabilidades y la rendición de cuentas de los operadores de IC e ICI, así como los canales de comunicación y los mecanismos de cooperación entre los organismos públicos y privados para garantizar la operación y recuperación de los servicios e infraestructuras críticos.

5.23 Definir bases mínimas de ciberseguridad

La Estrategia debe poner de relieve los marcos legislativos y reglamentarios existentes o proponer el desarrollo de nuevos marcos, que describan las bases mínimas de ciberseguridad para los operadores de IC e ICI. Las bases de seguridad deben abordar una serie de prioridades de gestión de riesgos de alto nivel, así como prácticas de ciberseguridad más específicas. En el desarrollo de las bases deben considerarse las normas y las mejores prácticas reconocidas internacionalmente para garantizar mejores resultados en materia de seguridad y una mayor eficiencia.

5.24 Utilizar una amplia gama de políticas de mercado

La Estrategia debe tener en cuenta una amplia gama de políticas para garantizar que todas las organizaciones y personas estén realmente incentivadas a cumplir sus responsabilidades individuales en materia de ciberseguridad, en proporción con los riesgos a los que se enfrentan.

Identificar las brechas entre lo que los mercados pueden y deben impulsar y lo que requiere el entorno de riesgo, es un paso crucial para determinar cuándo y cómo aprovechar la gama de incentivos y desincentivos disponibles para mejorar la seguridad.

5.25 Establecer asociaciones público-privadas

La Estrategia debe fomentar la creación de asociaciones formales entre los sectores público y privado para aumentar la seguridad de las IC y las ICI. Las asociaciones público-privadas son una piedra angular para proteger eficazmente las infraestructuras críticas y gestionar los riesgos de seguridad tanto a corto como a largo plazo.

Reconociendo que la ciberseguridad es una responsabilidad compartida, se pueden considerar métodos de colaboración como serian la asociación entre múltiples partes interesadas y la asociación público-privada. Estas asociaciones se pueden definir como *diferentes actores sociales que trabajan juntos, comparten riesgos y combinan recursos y competencias únicos para abordar desafíos o explotar oportunidades de maneras que uno no puede lograr solo*. Aquí se identifica como una asociación donde el sector público, el sector privado, la sociedad civil y la academia trabajan juntos como iguales a través de un compromiso organizado y de largo plazo para contribuir por un bien común. Los puntos destacables bajo estas definiciones son la diversidad de actores, la igualdad entre ellos, el reparto de riesgos y recursos y el logro de objetivos colectivos.

5.26 Capacitación, creación de competencias y sensibilización

Los elementos de esta área de interés abordan los desafíos relacionados con la capacitación en materia de ciberseguridad (a nivel individual e institucional) y la sensibilización entre las partes interesadas.

5.27 Planificar estratégicamente la capacidad y el desarrollo de capacidades y la sensibilización

La Estrategia debe asignar roles y responsabilidades claros a las entidades encargadas de coordinar la capacitación y sensibilización en materia de ciberseguridad. Estas entidades deben encargarse de identificar las brechas existentes en las necesidades de capacitación, las habilidades y la concienciación e informar sobre las soluciones prospectivas.

5.28 Desarrollar currículos de ciberseguridad

La Estrategia debe facilitar el desarrollo o la ampliación de planes de estudios escolares específicos destinados a acelerar el desarrollo de habilidades y la concientización en materia de ciberseguridad en todo el sistema educativo formal. Los planes de estudio deben ser interdisciplinarios y multidisciplinarios, y abarcar no solo habilidades y temas técnicos en materia de ciberseguridad. Además, deben tomar en cuenta la sensibilización tecnológica y su relación con los derechos humanos, el acceso a la información y la promoción de la justicia e igualdad dentro de la nación.

5.29 Estimular el desarrollo de capacidades y la capacitación de la fuerza laboral

La Estrategia debe fomentar el desarrollo de programas de formación y desarrollo de capacidades en ciberseguridad para expertos y no expertos de los sectores público y privado. También debe fomentar la formación específica de los agentes nacionales que participan en la política interior y exterior, incluidos los reguladores y los legisladores. Es recomendable avanzar hacia esquemas de

certificación y validación del conocimiento, acordes con estándares reconocidos internacionalmente, de manera tal que se asegure la posesión de las capacidades para enfrentar los desafíos.

5.30 Implementar un programa coordinado de sensibilización en materia de ciberseguridad

Las entidades responsables de las campañas y actividades de sensibilización sobre la ciberseguridad a nivel nacional deben colaborar con las partes interesadas pertinentes para elaborar y aplicar programas de sensibilización sobre la ciberseguridad centrados en la difusión de información sobre los riesgos y amenazas de la ciberseguridad, así como sobre las mejores prácticas para contrarrestarlos.

5.31 Fomentar la innovación, la investigación y el desarrollo en ciberseguridad

La Estrategia debe fomentar un entorno que estimule la investigación básica y aplicada en materia de ciberseguridad en todos los sectores y en los distintos grupos de las partes interesadas. Se debe prever el desarrollo de un mercado local eficiente y suficiente de servicios de ciberseguridad, y establecer vínculos con la comunidad internacional de investigación en los campos científicos relacionados con la ciberseguridad.

5.32 Adaptar los programas a los sectores y grupos vulnerables

La Estrategia debe identificar los grupos de la sociedad que requieren especial atención en lo que respecta a la capacitación y el desarrollo de capacidades en materia de ciberseguridad y la sensibilización. Es importante entender las posibilidades de uso de la tecnología, a través de encuestas y estudios que permitan diagnosticar el nivel de conocimiento del que se parta para diseñar instrumentos eficaces para la ejecución de programas y proyectos en esta materia.

5.33 Legislación y regulación

Esta área de interés aborda el desarrollo de un marco legal y regulatorio para proteger a la sociedad contra la ciberdelincuencia y promover un entorno cibernético seguro. Este marco debe incluir: la adopción de legislación que defina las actividades cibernéticas ilegales; la implementación de herramientas procesales para investigar y enjuiciar estos delitos a nivel nacional y en colaboración internacional; el establecimiento de mecanismos de cumplimiento; el fortalecimiento de la capacidad de aplicación; la institucionalización de entidades críticas y la cooperación global contra el ciberdelito. El marco también debe reconocer y ser coherente con las obligaciones del país en virtud del derecho internacional, regional y nacional de los derechos humanos. La Estrategia debe informar y orientar el desarrollo de la legislación, de modo que los roles y responsabilidades sean claros y estén bien definidos.

5.34 Establecer un marco jurídico nacional para la ciberseguridad

La estrategia debe fomentar el desarrollo de marcos jurídicos nacionales de ciberseguridad y protección de datos, que se refieran a las acciones pertinentes para la prevención, el seguimiento y la gestión de incidentes cibernéticos, y cualquier otra acción que las entidades públicas y privadas deban emprender para fomentar un ciberespacio nacional seguro y resiliente. La estrategia debe proporcionar orientación sobre cómo abordar los enfoques normativos comunes que afectan tanto a la ciberseguridad como a la ciberdelincuencia.

5.35 Establecer un marco jurídico nacional sobre la ciberdelincuencia y las pruebas electrónicas

La Estrategia debe promover el desarrollo de un marco jurídico nacional que defina claramente lo que constituye la ciberdelincuencia y los delitos penales conexos, y que otorgue facultades procesales adecuadas para la investigación y el enjuiciamiento eficaces, así como para la adjudicación de casos conexos sobre la base de pruebas electrónicas admisibles.

5.35 Reconocer y salvaguardar los derechos humanos y las libertades

La Estrategia debe promover el desarrollo de marcos jurídicos nacionales sobre ciberseguridad, ciberdelincuencia y otros ámbitos conexos que respeten y protejan los derechos humanos. La Estrategia debe prestar especial atención a las cuestiones jurídicas relacionadas con la tecnología que pueden afectar al nivel de ciberseguridad y que tienen repercusiones en los derechos humanos, y promover enfoques coherentes con los derechos humanos de las personas.

5.37 **Crear mecanismos de cumplimiento**

La Estrategia debería promover el establecimiento de mecanismos nacionales de cumplimiento que prevengan, combatan y mitiguen las acciones dirigidas contra la confidencialidad, integridad y disponibilidad de los sistemas e infraestructuras TIC, y que amenacen los datos informáticos, de acuerdo con el marco legal antes mencionado. Asimismo, debe fomentar la adopción de esquemas de auditoría y certificación de sistemas de gestión de seguridad de información basados en la norma ISO/IEC 27001 y para sistemas de control industrial para infraestructuras críticas basados en la norma IEC 62443.

5.38 **Promover el fomento de la capacidad de los organismos encargados de hacer cumplir la ley**

La Estrategia debe fomentar la capacitación en la aplicación de la ley en materia de ciberseguridad, dirigida a las partes interesadas que participan en la lucha contra la ciberdelincuencia.

5.39 **Establecer procesos interorganizacionales**

La Estrategia debe identificar y reconocer los mandatos de los organismos nacionales encargados de garantizar el cumplimiento de la legislación sobre delitos cibernéticos, incluyendo los responsables de la prevención y la respuesta a los incidentes cibernéticos, los responsables de garantizar que todos los requisitos internacionales en materia de delitos cibernéticos se cumplan y se extiendan a través de las fronteras judiciales.

5.40 **Apoyar la cooperación internacional para combatir las amenazas cibernéticas**

La Estrategia debe comprometerse a proteger a la sociedad contra la ciberdelincuencia que tiene un ámbito global que afecta a todos los países a escala mundial, mediante la participación en la construcción, de forma incluyente, de acuerdos internacionales sobre la ciberdelincuencia, así como para la promoción de mecanismos de coordinación internacional. La Estrategia debe reconocer la importancia de crear mecanismos informales que permitan la cooperación confiable y el oportuno intercambio internacional de información, inteligencia y apoyo técnico entre los actores de la ciberseguridad tanto en el sector público como en el privado. En esta área de interés, se hace hincapié en los elementos que la Estrategia debe abarcar en términos de compromisos en materia de ciberseguridad del país, tanto a nivel regional como internacional. La Estrategia debe reconocer

el carácter sin fronteras y la dimensión internacional de la ciberseguridad, y destacar la necesidad de que el país y sus organismos especializados participen en debates internacionales y cooperen con las partes interesadas nacionales e internacionales, así como con la sociedad civil, la industria y las organizaciones no gubernamentales.

Por lo anterior, la Estrategia debe incluir la participación en alianzas internacionales y la colaboración con instituciones académicas y organismos internacionales, como la Organización de los Estados Americanos, el Foro Global de Expertos en Ciberseguridad de la ONU y el Banco Mundial, para mejorar la transferencia de conocimiento, promover estándares internacionales y adoptar mejores prácticas en la capacitación y desarrollo de capacidades.

5.41 Reconocer la ciberseguridad como un componente de la política exterior y alinear los esfuerzos nacionales e internacionales

La Estrategia debe expresar un compromiso explícito con la cooperación internacional en materia de ciberseguridad y reconocer las cuestiones cibernéticas como un componente integral de la política exterior del país en todos los ámbitos pertinentes. Asimismo, la Estrategia debe establecer claramente las áreas de interés del gobierno e indicar los objetivos a largo plazo para la cooperación internacional, incluyendo qué partes interesadas participarían. Además, se debe garantizar la coherencia entre las agendas de política interna y exterior del país mediante la armonización de su marco jurídico y sus políticas nacionales con sus compromisos internacionales, y la armonización de sus enfoques nacionales de ciberseguridad con sus esfuerzos internacionales.

5.42 Participar en discusiones internacionales y compromiso con la implementación

La Estrategia debe identificar foros internacionales y mecanismos de cooperación específicos a los que el país desee unirse o con los que desee cooperar para participar de manera efectiva a nivel internacional en cuestiones relacionadas con la cibernética. La Estrategia debe especificar el compromiso del país con la aplicación del derecho internacional, incluida la Carta de las Naciones Unidas y la legislación internacional en materia de derechos humanos. La Estrategia también debe alentar el compromiso del país con la promoción de normas voluntarias de comportamiento responsable de los Estados en el ciberespacio y de las medidas de fomento de la confianza en el entorno digital.

5.43 Promover la cooperación formal e informal en el ciberespacio

La Estrategia debe indicar los mecanismos de cooperación internacional con los que el país desea comprometerse. La participación en esas iniciativas podría apoyar una mejor cooperación e intercambio de información oportuna y procesable entre las autoridades pertinentes sobre posibles amenazas y vulnerabilidades, así como la coordinación de los mecanismos de defensa y respuesta a contención de amenazas.

5.44 Promover el desarrollo de capacidades para la cooperación internacional

A medida que el país comience a emprender compromisos internacionales, es probable que estos requieran que el gobierno desarrolle competencias y habilidades adicionales centradas en cuestiones cibernéticas y aumente su capacidad general para abordar una gama cada vez mayor de problemas cibernéticos. Como consecuencia es importante fomentar el desarrollo y el uso de

competencias y capacidades centradas en cuestiones cibernética. La Estrategia también puede incluir el desarrollo de estructuras organizativas específicas y el establecimiento de alguna oficina dedicada o personal capacitado cuyo enfoque principal sea el compromiso diplomático en cuestiones cibernéticas relacionadas con el comercio, la diplomacia y el derecho internacional.

Fin de documento