CYBER4Dev

CAJA DE HERRAMIENTAS DE LA ESTRATEGIA NACIONAL DE **CIBERSEGURIDAD**

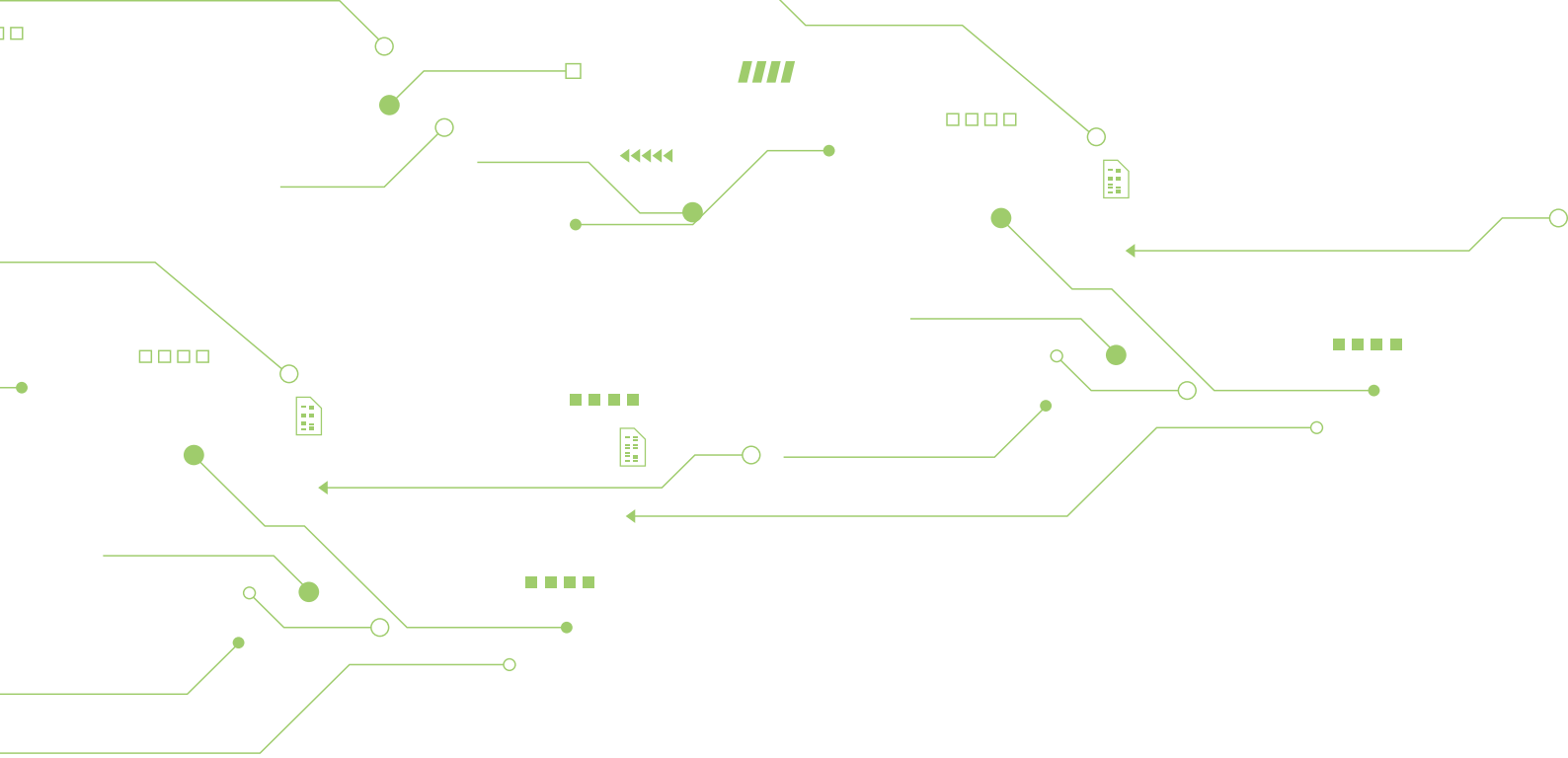
NI·CO

Republic of Estonia
Information System Authority

Foreign, Commonwealth & Development Office

Ministry of Foreign Affairs of the Netherlands

Funded by the European Union



Funded by the European Union

Este documento ha sido elaborado con la ayuda financiera de la Unión Europea. Las opiniones aquí expresadas no reflejan en modo alguno la opinión oficial de la Unión Europea.

Diseñada por **HUMAN Design Studios**

Kadri Kaska

Kadri Kaska es experta sénior en ciberseguridad en la Academia de Cibergobernanza (eGA), y sus principales áreas de especialización son la estrategia nacional de ciberseguridad y los marcos de gobernanza, así como la legislación nacional e internacional. Antes de incorporarse a la eGA en 2022, trabajó durante más de una década en el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCDCOE) como investigadora jurídica y política en materia de ciberseguridad y Jefa de la Sección Jurídica. Durante su estancia allí, estuvo destinada en la Autoridad de Sistemas de Información de Estonia, donde contribuyó a las actividades de la agencia en materia de evaluación de amenazas cibernéticas, análisis de políticas y redacción jurídica. Kadri ha sido la autora principal y editora de las evaluaciones anuales de ciberseguridad de Estonia, una de las autoras de la Ley de Ciberseguridad de Estonia y de la Estrategia de Ciberseguridad de 2018, y ha colaborado con varias organizaciones internacionales y regionales en el desarrollo de capacidades en materia de ciberseguridad. Kadri tiene un máster en Derecho por la Universidad de Tartu y actualmente cursa estudios de Ciencias del Comportamiento en la misma universidad.

Liis Rebane

Liis Rebane es una profesional de las TI y la seguridad de la información con más de cuatro años de experiencia práctica en gestión y control de riesgos de TI y seguridad en el sector financiero. Anteriormente, trabajó como Coordinadora Nacional de Ciberpolítica para Estonia, siendo responsable de la planificación y ejecución de la Estrategia Nacional de Ciberseguridad, además de contribuir a la adopción de la directiva NIS. En los últimos años, Liis ha colaborado con varios países en la elaboración de estrategias nacionales de ciberseguridad, la realización de evaluaciones de ciberseguridad y la organización de cursos de formación y talleres. Liis es doctora en física y cuenta con más de 10 años de experiencia en investigación académica y aplicación de métodos cuantitativos.

Índice

Visión general

El objetivo de esta caja de herramientas es ofrecer una guía concisa y práctica para crear o actualizar una Estrategia Nacional de Ciberseguridad (ENC). Su objetivo es ayudar a las autoridades nacionales en la ejecución del proceso de la ENC mediante la incorporación de lecciones prácticas, factores de éxito y errores comunes para garantizar la entrega oportuna de un documento completo y adaptado de la ENC, con una gobernanza sólida y una amplia participación de las partes interesadas.

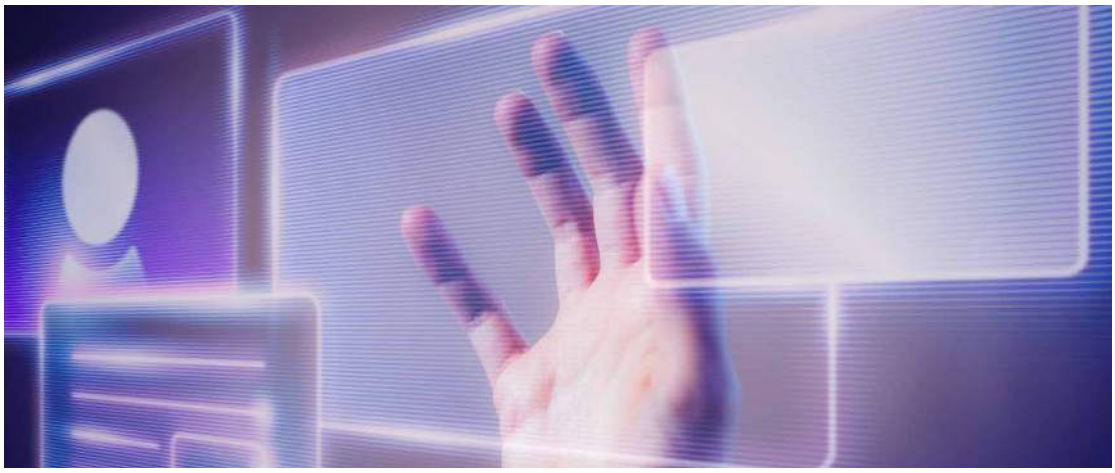
Basándose en la experiencia de los autores en la ejecución del proyecto Cyber4Dev, así como en sus funciones en las autoridades nacionales y como consultores de apoyo a los procesos de ENC en varios países, la caja de herramientas ofrece orientaciones prácticas y reales para el desarrollo de ENC. No sustituye a la literatura académica y política que ofrece una orientación exhaustiva sobre la teoría de las ENC, sino que presenta un enfoque honesto basado en las experiencias de los autores, centrado en un proceso pragmático de ENC que, aunque aspira a lo ideal, ha demostrado su eficacia en la práctica.

La caja de herramientas consta de dos partes principales:

1. En la Parte I, **Proceso de elaboración de una estrategia nacional de ciberseguridad (ENC),** se exponen los pasos y consideraciones prácticas esenciales para desarrollar una nueva ENC.

1. La Parte II, **Áreas temáticas de las ENC,** presenta una colección de "componentes básicos" de las ENC que deben tenerse en cuenta a la hora de desarrollar una ENC, centrándose en la ciberseguridad y la resistencia básicas.

La caja de herramientas concluye con consejos y observaciones generales basados en la experiencia de los autores, acompañados de una lista de directrices y herramientas internacionales de buenas prácticas en materia de ENC, que se consideran recursos valiosos y prácticos para obtener orientación y conocimientos detallados tanto sobre la configuración general de las ENC como sobre áreas estratégicas específicas.



Cómo utilizar este documento

Se recomienda a los usuarios de la caja de herramientas que sigan las etapas descritas en el Proceso ENC, refiriéndose a las Áreas Temáticas ENC para el establecimiento de objetivos, la priorización y el mapeo de las necesidades y compromisos de las partes interesadas.

El capítulo 1, **Proceso de la ENC,** identifica seis etapas esenciales para el éxito del diseño de una ENC:

1. **Definición de la propiedad del proceso ENC:** Designar una agencia líder y una junta consultiva para dirigir la ENC.
2. **Creación de un plan de proyecto ENC:** Elabore un calendario con hitos, resultados y responsabilidades claros.
3. **Evaluación del contexto estratégico:** Evaluar el panorama de amenazas, determinar la madurez actual y realizar un análisis DAFO.
4. **Identificacion de la visión y los principios rectores.**
5. **Desarrollo de objetivos estratégicos y líneas de acción.**
6. **Identificación y compromiso de las partes interesadas:** Involucrar a las partes interesadas de los sectores público y privado y establecer un enfoque claro para la participación de las partes interesadas durante las fases de redacción, validación y finalización.
7. **Perspectivas para los próximos pasos: Plan de acción y implementación de la ENC.**

Estas etapas forman una secuencia interconectada para los cimientos del documento y el proceso de la ENC. No obstante, las etapas deben revisarse de forma iterativa a medida que aumenta la participación de las partes interesadas, se profundiza en la comprensión y se aclara la visión estratégica.

El Capítulo 2, **Áreas temáticas de la ENC,** esboza los "bloques de construcción" clave para dar forma al contenido y la estructura de la ENC, abarcando la gobernanza de la ciberseguridad, la gestión de riesgos, las capacidades de gestión de incidentes y la concienciación y habilidades en ciberseguridad. El enfoque y la estructura de la ENC diferirán de un país a otro, en función de las necesidades, prioridades y madurez nacionales. No obstante, unas prácticas comunes pueden guiar el proceso inicial. La distinción de la caja de herramientas entre capacidades básicas y avanzadas ayuda a establecer prioridades realistas y a mantener un alcance manejable.

El Proceso ENC

Definición de la propiedad del proceso de ENC

El primer paso para el éxito de un proceso de ENC consiste en asignar la propiedad tanto personal como institucional y establecer una junta de supervisión y asesoramiento dedicada como mecanismo para conectar con las partes interesadas necesarias. A continuación, se ofrece una guía detallada para ejecutar este paso, que incluye el propósito, el papel y las tareas, consideraciones sobre recursos y recomendaciones.

Un proceso de ENC debe comenzar con la

designación **de una organización competente y una persona responsable del proceso de ENC,** idealmente a nivel gubernamental. El propietario de la ENC es responsable de desarrollar un plan de proyecto y dirigir la ejecución del proceso de desarrollo de la estrategia. Tanto la organización como el individuo deben tener la competencia en la materia, el mandato y los recursos adecuados para completar el proceso con éxito.

En la práctica, la elección óptima para este papel tiende a ser la organización responsable de la ciberseguridad del país o de la agenda de digitalización - el área que ostenta esta responsabilidad varía mucho de un país a otro, desde la economía o la educación, hasta la defensa militar o la seguridad interna. Aunque hay ejemplos más y menos exitosos en todo el espectro, es importante que la organización responsable sea capaz de involucrar ampliamente a las partes interesadas y comprenda el valor de la comunicación y el intercambio abierto de información, lo que puede suponer un esfuerzo consciente adicional si la responsabilidad de la ENC se asigna a una organización con cultura militar o de seguridad interna. Una ENC con un contenido sustancial debe ser un documento público para establecer el nivel necesario de compromiso en toda la sociedad. Puede establecerse un apéndice complementario no público o clasificado más detallado para cubrir contenidos más sensibles, si se identifica la necesidad de ello. Por último, es importante que la organización propietaria de la ENC tenga autoridad para exigir responsabilidades a otras organizaciones (al menos del sector público) por sus acciones en este ámbito. Si se carece de dicha autoridad, una entidad de nivel superior, como el ministerio de TIC, debería asumir la propiedad del proceso. Aunque esta organización tendrá la responsabilidad de producir la ENC, es esencial que involucre a un amplio abanico de partes interesadas gubernamentales y no gubernamentales en cada fase del proceso.

La consultoría externa puede ser beneficiosa para prestar apoyo a la organización responsable del proceso de ENC. Sin embargo, es importante tener en cuenta que la **apropiación en sí no puede externalizarse.** La ayuda de responsables, facilitadores y asesores experimentados puede ser inestimable, especialmente para los países que se encuentran en las primeras fases de un proceso maduro de ECN. Pueden aportar experiencia y capacidad adicionales, pero la responsabilidad última sigue recayendo en la organización designada.

A continuación, establezca **una junta de supervisión y asesoramiento** para el desarrollo de la estrategia, con el fin de garantizar la participación y las aportaciones adecuadas de las organizaciones dentro de sus áreas de gobierno. El consejo debería estar formado por representantes de todas las áreas temáticas de la estrategia, con miembros que posean tanto competencia en la materia como un mandato para representar las necesidades y prioridades de sus organizaciones. Además de una amplia representación de la organización gubernamental, resulta útil considerar la representación del sector privado, las ONG y el mundo académico para garantizar la participación directa de las múltiples partes interesadas. Alternativamente, las aportaciones de las partes interesadas no gubernamentales pueden incorporarse a través de talleres, entrevistas y rondas de retroalimentación.

La junta consultiva actúa como principal caja de resonancia para las decisiones importantes relativas a la estrategia. Debe ser informado periódicamente sobre el estado de los trabajos, las necesidades y los resultados. Es importante que todos los miembros de esta junta se comprometan con las organizaciones, incluidos el sector privado, la sociedad civil y el mundo académico, dentro de sus áreas de gobierno, para proporcionar los aportes y comentarios necesarios para la estrategia

Creación de un plan de proyecto ENC

Una vez definido el propietario del proceso, el primer paso esencial es redactar un plan de proyecto para el proceso de desarrollo de la estrategia y coordinarlo con la junta consultiva. La aprobación formal por parte de la junta puede ser beneficiosa, dependiendo de la tradición administrativa y la cultura del país, pero no es esencial. Sin embargo, el plan del proyecto debe contar al menos con su apoyo, considerando adecuadamente sus necesidades y garantizando su compromiso de ejecución. De lo contrario, existe el riesgo de que les tome por sorpresa y no se comprometan suficientemente con el proceso.

Una ENC debe tener una duración determinada, tras la cual debe iniciarse una revisión y desarrollo de la nueva ENC. Incluso la estrategia mejor elaborada se verá afectada por la evolución del panorama externo de amenazas y riesgos, las nuevas tecnologías, los cambios geopolíticos y otros factores. Entre cinco y ocho años es un plazo razonable para una estrategia; tiempo suficiente para fijar la dirección estratégica, pero no demasiado para que resulte redundante.

El plan del proyecto podría tener en cuenta los elementos enumerados en el ejemplo de plan de proyecto que se ofrece a continuación. Las tareas se detallarán en secciones posteriores del documento.

Tenga en cuenta que el cronograma indicativo propuesto en el cuadro debe considerarse el mínimo posible: se basa en la práctica real, pero refleja el proceso en circunstancias casi ideales (equipo comprometido, número reducido de partes interesadas y comunicación eficaz). Dependiendo del alcance de las organizaciones implicadas y de la complejidad de la situación, el proceso podría llevar bastante más tiempo.

Tarea	Responsabilidad	Producto(s) final(es)	Cronología
Inicio del proyecto			
Establecer el propietario y líder del proyecto		Propietario del proyecto y líder designado	Mes 1
Validación del proyecto con la Junta Consultiva	Propietario/líder del Proyecto	Miembros de la Junta Consultiva	Mes 1
	Miembros de la Junta Consultiva	POC asignados desde las organizaciones de la Junta Consultiva	Mes 1
Evaluación inicial (informe y estructura)	Propietario/líder del proyecto	Evaluación entregada y presentada a la Junta Consultiva	Meses 1-2
Compromiso de las partes interesadas			
Taller inicial con las partes interesadas	Propietario/líder del proyecto (se recomienda apoyo externo para la facilitación y documentación)	Taller inicial con las partes interesadas: establecer el compromiso de las partes interesadas con el proceso y el cronograma de la ENC y documentar los comentarios iniciales.	Mes 2
Entrevistas/ consultas con las partes interesadas	Propietario del proyecto con miembros del equipo o apoyo externo	Aportaciones documentadas al proceso estratégico por parte de todos los principales grupos interesados.	Meses 2-3

Tarea	Responsabilidad	Producto(s) final(es)	Cronología
Proyecto de estrategia			
Primer borrador de la estrategia y consulta con el consejo consultivo (1-2 ciclos)	Redacción por parte del propietario del proyecto (puede considerarse la posibilidad de contar con apoyo externo para apoyar a la parte interesada en el proceso de redacción). Participación de las partes interesadas con el apoyo de los miembros de la Junta Consultiva	Proyecto inicial de estrategia, que incorpora las aportaciones de las consultas a las partes interesadas. Periodo de revisión de 3 semanas para las partes interesadas nacionales, que dio lugar a una ronda exhaustiva de comentarios y aportes iniciales.	Mes 3
Incorporar las reacciones al proyecto de estrategia.	Propietario del proyecto	Segundo borrador de la estrategia	Mes 4
Consulta			
Taller de validación con las partes interesadas	Propietario del proyecto (se recomienda apoyo externo para la facilitación)	Revisión común y alineación con las principales partes interesadas	Mes 4
Periodo de revisión nacional	Propietario del proyecto con el apoyo del consejo asesor	Validación y respuesta por escrito a la estrategia por parte de todas las partes interesadas nacionales (aproximadamente 1 mes).	
Revisión y alineación	Propietario del proyecto (posiblemente con apoyo externo)	Concluir el proyecto final	Mes 5

Tarea	Responsabilidad	Producto(s) final(es)	Cronología
Finalización			
Finalización y aprobación	Propietario del proyecto con el apoyo de la Junta Consultiva	Alineación final del borrador entre las principales partes interesadas. Iniciar el proceso de adopción nacional	Mes 6
Presentación para adopción	Propietario del proyecto	Presentación de la ENC final	Mes 7

Evaluación del contexto estratégico

La mejora de la ciberresiliencia nacional requiere comprender el estado actual y la perspectiva estratégica de la ciberseguridad, abarcando factores externos (panorama de ciberamenazas) e internos (capacidad nacional). Un análisis FODA, las consultas con las partes interesadas y la referencia a las mejores prácticas internacionales pueden servir de guía. Sin embargo, para tener éxito como medio para lograr el cambio, una estrategia debe tener en cuenta el contexto nacional. Un enfoque único que no tenga en cuenta los factores específicos de cada país no será tan eficaz.

El contexto nacional viene determinado por varios factores, no todos ellos directamente relacionados con la ciberseguridad:

- ¿Cuál es la estructura administrativa existente, la tradición, los límites constitucionales? ¿Dónde recaería de forma más natural la responsabilidad en materia de ciberseguridad? ¿Cómo se asigna la autoridad decisoria y a qué nivel?
- ¿Cuál es la cultura de toma de decisiones predominante en el país? El punto de equilibrio entre subordinación y colaboración puede variar mucho de un país a otro. En una cultura descendente, pueden ser necesarias iniciativas políticas para mejorar horizontalmente la cooperación público-privada, por ejemplo.
- ¿Cuáles son los objetivos nacionales relacionados con la digitalización? ¿Cuáles son los objetivos en otros ámbitos con los que conectará la ciberestrategia: implementación de la ley, desarrollo económico, defensa nacional, asuntos exteriores?

Análisis FODA de la ciberseguridad

El propósito de este ejercicio es identificar las oportunidades y retos existentes que informan el proceso de estrategia. El análisis no forma parte necesariamente del documento de estrategia, pero el balance es crucial para determinar en qué punto se encuentra el país e informar sobre la definición de hacia dónde le gustaría ir.

- **Oportunidades:** Beneficios que el país espera de la transformación digital y la ciberseguridad; dinámicas recientes que

ponen de relieve problemas y tendencias acuciantes (por ejemplo, cambios en el patrón de trabajo inducidos por COVID).

- **Amenazas:** Panorama regional y nacional de las ciberamenazas, actores clave de las amenazas, incidentes recientes significativos; dependencia general y específica de las TIC (por ejemplo, dependencia excesiva de proveedores únicos, tecnología heredada o no fiable); sectores de alto riesgo debido a su importancia social y económica en los que la interrupción del servicio acarrearía consecuencias graves o a gran escala.
- **Fortalezas:** estructuras existentes, organizaciones, mandatos, legislación, oferta y acceso al talento.
- **Debilidades:** Capacidades y recursos organizativos; concienciación sobre ciberseguridad entre los grupos destinatarios y la población en general; nivel de implicación en la cooperación internacional.

Identificación de la visión y los principios rectores

Una visión coherente y unos principios fundamentales apoyan la alineación estratégica a largo plazo: son puntos de anclaje que ayudan a orientar tanto hacia dónde (visión) y cómo (valores) desea avanzar el país. Para que la visión y los principios fundamentales sirvan a este objetivo, deben ser: a) orgánicos al contexto del país y a las partes interesadas, b) fáciles de recordar, y c) ofrecer inspiración y claridad a la hora de navegar entre decisiones.

Desarrollar una visión y unos principios rectores forma parte del proceso de la ENC tanto como la definición de los objetivos estratégicos y el acuerdo sobre las líneas de actuación. Deben diseñarse en colaboración y consulta con las partes interesadas. Sugerimos utilizar la visión y los principios de la ENC para vincular la ciberseguridad al sistema de valores nacionales más amplio (por ejemplo, inclusión, apertura, competitividad, confianza y fiabilidad) y evitar declaraciones de visión demasiado vagas, largas o inverosímiles[1].

Aunque las referencias internacionales ofrecen principios rectores para el proceso de la ENC[2], los siguientes son los que más han calado en nuestra experiencia de proyecto:

1 Para recomendaciones sobre una visión para la ENC, véase https://ncsguide.org/the-guide/principles/. Para recomendaciones sobre las características de una buena visión, véase https://www.sitra.fi/en/blogs/seven-tips-for-vision-creators/.

2 https://ncsguide.org/the-guide/principles/.

- **La ciberseguridad es un asunto de toda la sociedad y un elemento integral de la seguridad pública,** con responsabilidades conjuntas y compartidas de socios públicos y privados.
- **Promover el liderazgo y la colaboración:** involucrar activamente a las partes interesadas en la mejora de las condiciones del ciberespacio; comprometerse a participar activamente en la cooperación regional e internacional.
- **Salvaguardar y promover los derechos humanos y las libertades fundamentales tanto** en línea como fuera de ella, como la privacidad, la libertad de expresión y la libre circulación de la información.
- **Tener un enfoque basado en valores:** adhesión a los valores fundamentales de la sociedad: democracia, Estado de Derecho, transparencia y confianza pública a la hora de diseñar medidas de ciberseguridad; uso de instrumentos políticos apropiados que sean adecuados, eficaces y proporcionados; fomento de la diversidad (de género y de otro tipo) para aprovechar todo el potencial de talento.
- **Tratar la ciberseguridad como facilitadora y amplificadora del desarrollo digital y la prosperidad socioeconómica,** apoyando la innovación, la competitividad, el desarrollo sostenible y la inclusión social.
- **Tener un enfoque basado en el riesgo,** reconociendo que la seguridad absoluta no es alcanzable y promoviendo una resistencia que evite que los ciberriesgos tengan efectos adversos significativos en la sociedad y la economía..

Definición de objetivos estratégicos y líneas de acción

La definición de los objetivos estratégicos y las respectivas líneas de acción para alcanzarlos constituye el núcleo del documento y el proceso de la ENC que define el alcance previsto y la priorización de esfuerzos durante el periodo de la estrategia. En la sección "Áreas temáticas de la ENC" se detallan las orientaciones explícitas para elaborar el contenido y el borrador de las áreas temáticas que enmarcarán los objetivos y las líneas de actuación.

Los mayores retos para elegir y diseñar con éxito un conjunto de objetivos estratégicos junto con las acciones necesarias para cumplirlos son de naturaleza universal, independientemente del país o el sector:

- **Concluir objetivos estratégicos y líneas de acción desajustados, de modo** que la realización de las acciones no aporte el valor estratégico previsto.
- **Proceso de estrategia desconectado de la planificación de recursos:** este reto se intensifica en los países con un modelo de gobernanza nacional y descentralizado para la ciberseguridad.
- **Insuficiente conexión e integración entre la estrategia nacional de seguridad y otros documentos nacionales de planificación estratégica:** esto puede dar lugar a esfuerzos aislados en el ámbito de la ciberseguridad, que no están respaldados por esfuerzos de desarrollo más amplios y prioridades nacionales, lo que da lugar a resultados débiles y a un compromiso insuficiente a nivel nacional. Dado que la ciberseguridad se está convirtiendo en parte integrante de todos los ámbitos de la gobernanza y la planificación política a nivel nacional, la necesidad de una estrecha integración

no hará sino intensificarse con el tiempo.

- **No reconocer las limitaciones siempre presentes impuestas por los recursos humanos y financieros disponibles.** El reto se ve intensificado por la observación de que un proceso de planificación de una ENC tiende a comenzar siempre con una fuerte intuición inicial de que todo es importante y puede saltarse el paso de entablar un difícil debate sobre lo que *no* hay que hacer y priorizar durante el siguiente periodo de estrategia, lo que conduce a una estrategia vaga y a una priorización arbitraria

Si no se superan estos retos durante la fase de diseño de la ENC -en particular, garantizando un orden de prioridades suficiente, una asignación de recursos realista y la aceptación de las partes interesadas-, la pertinencia de la ENC puede verse limitada.

Participación de las partes interesadas y consultas

Para garantizar que la ENC sea pertinente en cuanto al fondo y establezca la apropiación y la rendición de cuentas, es crucial mantener estrechas consultas con un amplio abanico de partes interesadas. Estas consultas ayudan a recopilar información sobre el proyecto de estrategia, sus prioridades y acciones previstas, a verificar su calibración y pertinencia durante las rondas de comentarios, y a garantizar una amplia legitimidad y el compromiso de las partes interesadas, lo que resulta esencial para la posterior ejecución de las iniciativas estratégicas.

La lista típica de las principales partes interesadas podría incluir:

- Líderes gubernamentales en política digital y ciberseguridad
- Otros ministerios (incluidos los que desempeñan funciones menos obvias o menos directas en materia de ciberseguridad, como los de Justicia, Educación, Hacienda, Empresa, Defensa o Asuntos Exteriores).
- Organismos públicos con responsabilidades en materia de digitalización y ciberseguridad; reguladores sectoriales; autoridades policiales, de seguridad nacional y de defensa; proveedores de servicios clave dependientes de las TIC en la Administración y el sector público.
- Entidades del sector privado: proveedores de servicios de telecomunicaciones e Internet, otras entidades de infraestructuras nacionales críticas y organizaciones industriales.
- Instituciones educativas y de investigación
- Representantes de la sociedad civil y ONG que promueven la alfabetización informática
- Expertos individuales en TIC y cibernética

Además, se podrá recurrir a organizaciones y consultores internacionales y regionales para garantizar la armonización con las mejores prácticas y tendencias generales.

Los siguientes principios rectores han resultado útiles para planificar las consultas con las partes interesadas:

- Comprométase en función de las funciones necesarias, no sólo de las instituciones.
- Lo ideal sería contar con representantes de alto nivel, conocedores de las cuestiones de fondo de su área

- Equilibrar la representación formal con responsables de la toma de decisiones y expertos apasionados por el tema y capaces de impulsar el cambio.
- Incluir a visionarios del gobierno, el sector privado y el mundo académico.
- Distinga entre partes interesadas y espectadores: aunque una amplia retroalimentación es beneficiosa, no todas las opiniones tienen el mismo peso..

Lo más importante es asegurarse de que el compromiso es auténtico: dejar tiempo suficiente para hacer aportaciones y comentarios, y demostrar que se están teniendo en cuenta. Sea transparente y justifique si no se aceptan las propuestas. Si las partes interesadas no se comprometen con respeto y transparencia, pueden perder credibilidad con el tiempo.

Aconsejamos llevar a cabo varias rondas de consultas con las partes interesadas, utilizando formatos de reuniones y talleres tanto presenciales como en línea. La experiencia dice que lo mejor es aspirar a un grupo de tamaño medio (10-20 participantes) por consulta. Los participantes ideales son los que tienen el nivel suficiente para representar la posición de sus organismos, pero al mismo tiempo son lo bastante prácticos como para conocer las cuestiones de fondo.

El borrador final de la ENC debe someterse a consulta nacional para su revisión y retroalimentación. Es de esperar que la consulta nacional final aporte comentarios sustanciales: el responsable del proceso de la ENC, con el apoyo de recursos internos o externos, debe prepararse para revisar numerosos comentarios. Una tabla de coordinación puede ser útil para hacer un seguimiento de todos los comentarios y ofrecer garantías a todas las partes interesadas, indicando las razones para omitir cualquier comentario de la estrategia final. A menudo, puede haber comentarios demasiado detallados para el documento de estrategia, pero que aportan información valiosa para el posterior desarrollo del plan de acción para la implementación de la estrategia.

Próximos pasos: Plan de acción e implementación de la ENC

Una vez concluido el documento de estrategia de la ENC, es necesario establecer y seguir un ciclo de vida completo de la ENC, que comprende cuatro fases, como se detalla en la figura siguiente:

- Desarrollo de la estrategia
- Implementación de la estrategia
- Supervisión
- Revisión posterior a la implementación y lecciones aprendidas.

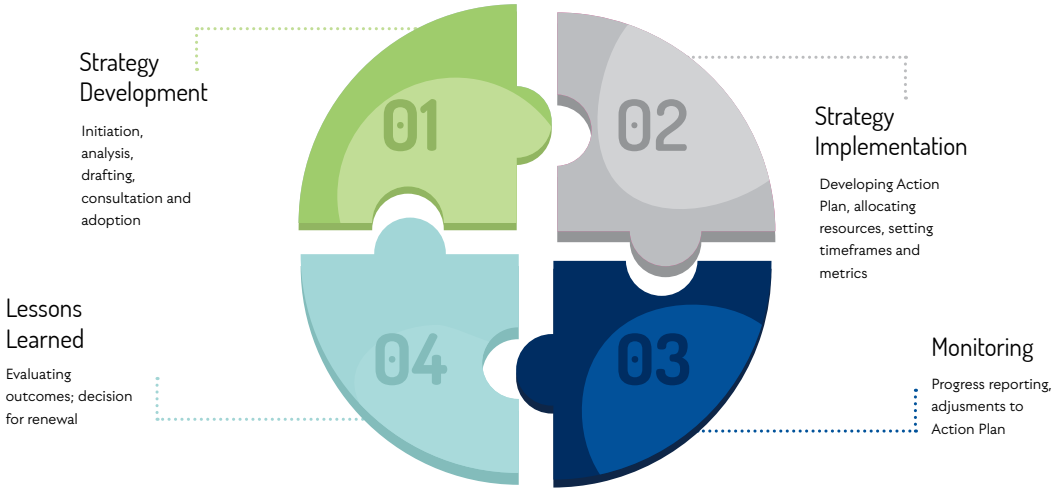
La caja de herramientas actual se centra en la fase de desarrollo de la estrategia, mientras que las orientaciones detalladas sobre la conclusión del plan de implementación, el seguimiento y la revisión posterior a la implementación quedan fuera del alcance de estas orientaciones.

Breve resumen de las etapas que siguen al desarrollo de la ENC:

Una vez concluida la ENC, es necesario elaborar un Plan de Acción complementario. Las estrategias carecen de valor si no se ponen en práctica, por lo que el Plan de Acción está ahí para garantizar que las tareas se lleven a cabo a tiempo y que la ENC se aplique con eficacia. Un Plan de

Acción debe contener tareas específicas, aclarar quiénes son los responsables y quiénes contribuyen a ellas, establecer plazos y parámetros de rendimiento para las entidades responsables, y trazar una hoja de ruta para las tareas estratégicas esbozadas en la ENC. El éxito de la implementación de un Plan de Acción también requiere una estructura de información que permita hacer un seguimiento de la implementación del Plan de Acción, de los avances logrados y de los posibles obstáculos. Dichos informes orientan sobre los ajustes necesarios en la implementación de la Estrategia, basándose en la evolución del panorama de amenazas y riesgos y teniendo en cuenta los cambios administrativos o de otro tipo pertinentes y la armonización con otros ámbitos estratégicos.

Una vez finalizado el periodo de la estrategia, deberá programarse un ejercicio de revisión posterior a la implementación y de lecciones aprendidas. De este modo se revisarán los progresos realizados en relación con los objetivos de la estrategia, se identificarán las lagunas existentes y se extraerán conclusiones valiosas para el diseño y la implementación de la siguiente estrategia. Lo ideal sería que este proceso de revisión incluyera un escrutinio independiente. Puede tratarse de personas de dentro o fuera del gobierno, pero para garantizar la imparcialidad no deben haber participado directamente en la implementación de la estrategia.



Áreas temáticas ENC

Esta parte de la caja de herramientas ofrece un ejemplo de lista de comprobación de temas y medidas a tener en cuenta para desarrollar los objetivos y líneas de actuación de la ENC, basándose en la experiencia del proyecto Cyber4Dev.

La ENC tiene por objeto lograr una mejora coherente de la capacidad nacional en materia de ciberseguridad abordando tanto cuestiones transversales como sectoriales.

Para ayudar a organizar el desarrollo de la ENC, esta caja de herramientas adopta un enfoque orientado a la línea de base, centrándose en las capacidades nacionales fundamentales que preceden a objetivos y madurez más avanzados. Este enfoque de referencia no pretende en modo alguno limitar la inclusión de otras áreas de interés, y varias referencias internacionales enlazadas al final de este documento proporcionan recursos y

conocimientos útiles para ello.

Hemos estructurado los objetivos y líneas de actuación fundamentales de la ENC en torno a bloques horizontales (transversales) y verticales (orientados a sectores). Este enfoque ayuda a desarrollar y sincronizar los contenidos de la ENC y garantiza que los objetivos sigan siendo manejables y coherentes. Estos bloques básicos incluyen:

1. Marco de gobernanza de la ciberseguridad
2. Marco de gestión de riesgos cibernéticos
3. Gestión nacional de ciberincidentes
4. Concienciación y educación sobre ciberseguridad

La profundidad y ambición de los objetivos dentro de cada bloque deben ajustarse a las necesidades, prioridades y madurez nacionales, así como a la disponibilidad de recursos. Así pues, los bloques pueden reorganizarse e incluirse otras áreas en función de las circunstancias nacionales. No obstante, para facilitar la gestión, recomendamos limitar la estrategia nacional a unas pocas áreas (hasta 5) con 3-5 objetivos cada una, con un total de no más de 12-15 objetivos para el periodo de la estrategia.

A la hora de sustanciar cada uno de estos bloques con objetivos y líneas de actuación a través del proceso y el documento ENC, hemos utilizado un enfoque en tres pasos:

1. **Presentar el contexto:** Incluye una breve descripción del entorno actual relevante para el área en cuestión. Destaca las tendencias nacionales e internacionales clave, los mecanismos organizativos existentes, los marcos jurídicos/normativos y los principales retos percibidos sobre la base de la evaluación estratégica.

2. **Definir un planteamiento claro del problema:** Esto implica articular retos y oportunidades específicos, que proporcionen una comprensión común de la pregunta "¿qué problema estamos resolviendo?". Los problemas identificados deben ser abordados directamente por los Objetivos y las Líneas de Acción. De este modo se garantiza que todas las cuestiones importantes estén vinculadas a una acción prevista, y que no se lleve a cabo ninguna actividad sin una justificación subyacente clara.

3. **Esbozar los objetivos estratégicos:** Este paso incluye las principales líneas de actuación y actividades prioritarias, reflejando ambiciones y compromisos alcanzables al final del periodo de la estrategia.

La estructura de los componentes básicos de una ENC se ilustra en el cuadro siguiente.

GOBERNANZA DE LA CIBERSEGURIDAD

Marco de gobernanza de la ciberseguridad

Mecanismos de cooperación entre las partes interesadas

Marco jurídico

Cooperación internacional

GESTIÓN DEL RIESGO CIBERNÉTICO

Identificación de las funciones y operadores nacionales ciberdependientes críticos

Evaluación de riesgos cibernéticos y marco de resistencia

Preparación ante las crisis a nivel de entidad/operador y nacional

GESTIÓN NACIONAL DE CIBERINCIDENTES Y LUCHA CONTRA LA CIBERDELINCUENCIA

Capacidades nacionales de prevención y respuesta ante ciberincidentes

Evaluación de amenazas y conocimiento de la situación

Lucha contra la ciberdelincuencia

EDUCACIÓN Y CONCIENCIACIÓN SOBRE CIBERSEGURIDAD

Aumentar la concienciación sobre ciberseguridad
Ciberseguridad en todos los niveles educativos
Personal calificado en ciberseguridad

Las siguientes secciones ofrecen un resumen breve y consolidado de los aspectos considerados por Cyber4Dev durante los proyectos de consultoría de ENC, que pueden servir como punto de partida para el desarrollo de ENC.

Gobernanza de la ciberseguridad

A la hora de establecer o perfeccionar el marco nacional de gobernanza de la ciberseguridad, hay ciertos aspectos fundamentales que deben tenerse en cuenta: establecer o reforzar las autoridades nacionales competentes en materia de ciberseguridad; asignar funciones y responsabilidades claras en materia de ciberseguridad a los gobiernos y otras partes interesadas; garantizar mandatos adecuados de supervisión y rendición de cuentas; y establecer marcos y foros para una coordinación y colaboración eficaces. Dependiendo de las necesidades nacionales, el estado de madurez y la ambición, pueden ser necesarios diferentes instrumentos políticos, por lo que a menudo también puede ser apropiado abordar en este bloque una amplia revisión legislativa.

Marco de gobernanza de la ciberseguridad

- Asignar responsabilidades ejecutivas de alto nivel en materia de ciberseguridad.
- Designar y dotar de recursos a la(s) autoridad(es) nacional(es) competente(s)

en materia de ciberseguridad.

- Formar un órgano intragubernamental de coordinación estratégica o de toma de decisiones.
- Definir las funciones y responsabilidades de otros actores gubernamentales en materia de ciberseguridad.
- Establecer la supervisión de la implementación de la ENC e implantar mecanismos regulares de supervisión y notificación de los indicadores de ciberseguridad..

Cooperación entre las partes interesadas

- Desarrollar un mecanismo de asociación público-privada en el que participen las partes interesadas.
- Crear plataformas de participación para la consulta política, la coordinación de actividades y la cooperación operativa.

Marco jurídico

- Realizar una evaluación del marco jurídico actual; identificar y aplicar los cambios legislativos necesarios para los objetivos de la ENC.
- Definir las funciones y responsabilidades nacionales en materia de ciberseguridad en el marco jurídico y reglamentario.

Cooperación internacional

- Identificar las principales plataformas internacionales y regionales de ciberdiplomacia; establecer un plan para desarrollar la capacidad de participar y representar a la nación en estas plataformas.
- Identificar la política regional e internacional de ciberseguridad, el intercambio de información y los formatos de cooperación operativa y planificar la conexión con ellos..

Marco de gestión de riesgos cibernéticos

El enfoque estratégico nacional para gestionar los riesgos cibernéticos debe abarcar, como mínimo, todas las funciones críticas para el funcionamiento del Estado y la sociedad. Este bloque incluye acciones relacionadas con la evaluación de los riesgos de ciberseguridad, la identificación de los activos dependientes de lo digital que determinan el funcionamiento tanto de los poderes del Estado como de los servicios críticos del sector privado, y la implementación de controles de seguridad adecuados para mitigar esos riesgos, así como la integración con la planificación de crisis. Una vez más, podría ser necesario planificar y aplicar cambios legislativos para aplicar adecuadamente las actividades de gestión de riesgos.

Identificación de funciones y operadores críticos dependientes de la ciberseguridad

- Desarrollar criterios y un marco jurídico para identificar a los operadores de infraestructuras críticas de información (ICI) y crear un catálogo completo de todos los operadores de ICI, mantenido y actualizado periódicamente.

- Establecer una norma común de ciberseguridad obligatoria para las instituciones gubernamentales y los operadores de ICI, siguiendo un enfoque basado en los riesgos y dando prioridad a la continuidad de los servicios esenciales.

Evaluación de riesgos cibernéticos y marco de resistencia

- Establecer normas de referencia, directrices y estrategias de auditoría nacionales para apoyar la implementación de medidas de ciberseguridad por parte de los operadores de ICI y exigirles responsabilidades por su cumplimiento. Priorizar las medidas e inversiones en función del perfil de riesgo nacional.
- Promover la supervisión continua de los riesgos a nivel nacional y fomentar la adopción de las mejores prácticas de ciberseguridad entre las entidades gubernamentales y del sector privado.
- Establecer un mecanismo de divulgación periódica de vulnerabilidades y de intercambio de información entre los operadores de infraestructuras críticas de información (ICI) y las autoridades competentes en materia de ciberseguridad.
- Establecer una práctica sistemática de identificación y desarrollo de escenarios de riesgo cibernético a nivel de operador y nacional que puedan proporcionar información para la planificación de crisis, pruebas de estrés y diseño de ejercicios, y los esfuerzos de gestión de la continuidad del negocio.

Gestión nacional de ciberincidentes y lucha contra la ciberdelincuencia

Los componentes básicos abordados en este bloque de construcción de la ENC son una capacidad funcional de prevención y respuesta a incidentes a nivel nacional en todo el espectro de las ciberamenazas, considerando también las capacidades de implementación de la ley para luchar mejor contra la ciberdelincuencia. En una ENC típica, la respuesta a incidentes y la implementación de la ley se abordarán probablemente en capítulos diferentes, pero ambos comparten varias similitudes: la necesidad de invertir en capacidades tanto preventivas como reactivas, la necesidad de una base jurídica clara y adecuada para la ejecución de los poderes del Estado, y una dimensión de cooperación internacional fuerte y de importancia fundamental. Este esbozo también podría ser útil para tenerlo en cuenta en el contexto del desarrollo de las capacidades nacionales de ciberdefensa, es decir, para prevenir y responder a las ciberamenazas relevantes para la seguridad y la defensa nacionales.

Capacidades nacionales de prevención y respuesta ante ciberincidentes

- Establecer un Equipo de Respuesta a Incidentes de Seguridad Informática/ Equipo de Respuesta a Emergencias Informáticas (CSIRT/CERT) con responsabilidad nacional para gestionar las amenazas y los incidentes de ciberseguridad. Establecer su papel como principal punto de contacto para notificar incidentes cibernéticos.
- Establecer una cartera de servicios fundamentales de CSIRT/CERT, tanto

proactivos como reactivos, para la prevención y respuesta ante incidentes cibernéticos.

- Establecer canales de comunicación seguros y de confianza de CSIRT/CERT para la comunicación y la cooperación, así como políticas para el tratamiento de la información. Establecer, fomentar y salvaguardar la práctica de compartir información sobre vulnerabilidades, amenazas e incidentes.
- Desarrollar criterios para evaluar los incidentes cibernéticos en función de su impacto en los activos críticos, los servicios y la población.

Preparación ante las crisis

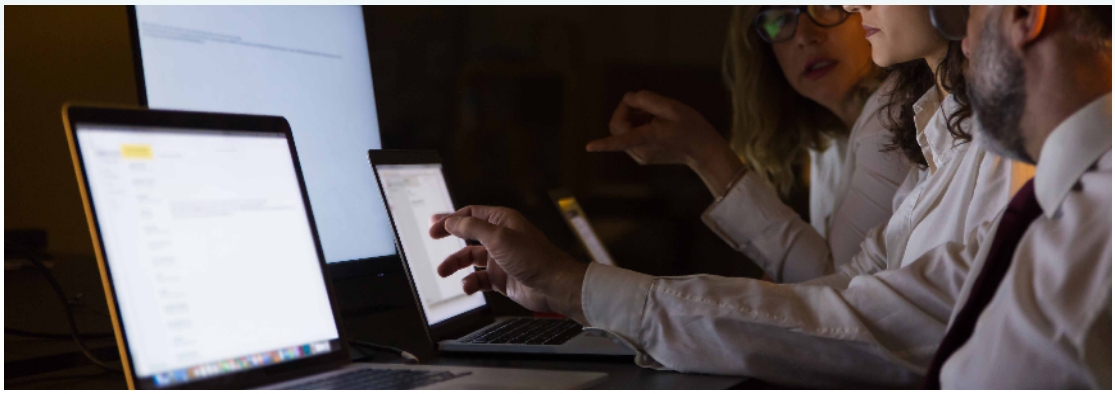
- Desarrollar planes de gestión de crisis para que las instituciones gubernamentales y el sector privado puedan hacer frente a las crisis cibernéticas. Organizar ejercicios nacionales de ciberseguridad para comprobar la eficacia de estos planes.
- Desarrollar un plan nacional de contingencia para prepararse ante incidentes o amenazas cibernéticas a gran escala, definiendo criterios de escalada, funciones de gestión de emergencias y planes de comunicación.
- Poner a prueba periódicamente el plan de contingencia cibernética mediante ejercicios a nivel operativo para perfeccionar los procesos de gestión de crisis y la toma de decisiones..

Evaluación de amenazas y conocimiento de la situación

- Evaluar periódicamente el panorama de amenazas y riesgos para fundamentar la toma de decisiones basada en riesgos y establecer actividades de concienciación y formación en ciberseguridad.
- Desarrollar un sistema de gestión del conocimiento para recoger las enseñanzas extraídas de los incidentes y las respuestas, respetando la confidencialidad empresarial.

Lucha contra la ciberdelincuencia

- Adoptar un marco jurídico para definir la ciberdelincuencia en armonía con los instrumentos internacionales.
- Establecer mandatos legales y autoridad para las fuerzas del orden, las autoridades ejecutivas y los proveedores de servicios digitales en la prevención de la ciberdelincuencia; definir las competencias de las fuerzas del orden y la fiscalía para la investigación de la ciberdelincuencia, incluida la recopilación de pruebas electrónicas y los mecanismos de cooperación internacional.
- Reforzar las capacidades judiciales y policiales con los recursos necesarios para una investigación eficaz de la ciberdelincuencia, incluidas las capacidades forenses digitales adecuadas, los procedimientos operativos normalizados y los mecanismos de denuncia de delitos publicados.
- Impartir formación a profesionales de la justicia penal sobre ciberdelincuencia, herramientas tecnológicas y gestión de pruebas electrónicas.



Concienciación y educación sobre ciberseguridad

El último pilar fundamental de la ENC se centra en establecer un enfoque global de la concienciación y la educación en materia de ciberseguridad para garantizar que todas las partes interesadas, incluidos los empleados de la Administración, los contratistas y el público en general, comprendan adecuadamente los riesgos cibernéticos y tengan la capacidad, las oportunidades y la motivación para adoptar un comportamiento seguro.

Aumentar la concienciación sobre ciberseguridad

- Crear un programa nacional coordinado de concienciación y cultura sobre ciberseguridad, que incluya un organismo coordinador para su implementación y gestión. Asignar recursos para la implementación a largo plazo del programa y definir métricas y rutinas para supervisar la concienciación en materia de ciberseguridad.
- Desarrollar programas de concienciación sobre ciberseguridad dirigidos a distintos grupos, como empresas, administraciones públicas, sociedad civil, población en general y jóvenes.
- Proporcionar directrices básicas de ciberseguridad fácilmente accesibles para ayudar a las organizaciones con recursos limitados; crear recursos de formación sobre ciberhigiene y gestión de riesgos para grupos clave, basados en objetivos pertinentes a nivel nacional.

Ciberseguridad en todos los niveles educativos

- Desarrollar un plan nacional de educación en ciberseguridad que defina las funciones y responsabilidades a todos los niveles del sistema educativo.
- Desarrollar recursos y herramientas para ofrecer conocimientos básicos de ciberhigiene en todos los niveles escolares.
- Integrar cursos de ciberseguridad en los programas de informática de la enseñanza superior.
- Crear programas de licenciatura y posgrado dedicados a la ciberseguridad para garantizar una oferta suficiente de talentos.

Personal calificado en ciberseguridad

- Preparar un programa de desarrollo de competencias para profesionales de organizaciones públicas.
- Realizar una evaluación nacional del déficit de competencias en ciberseguridad.
- Elaborar un plan de acción estratégico para el desarrollo a largo plazo de las competencias necesarias en materia de ciberseguridad.

Lecciones y observaciones generales

Esta sección resume las principales observaciones y recomendaciones generales de los autores para garantizar el éxito de la ENC.

La apropiación y el liderazgo coherente de la ENC son esenciales para el éxito. Hemos visto una y otra vez lo importante que es para el éxito del proyecto una dirección nacional comprometida, dedicada al proceso y con un mandato suficiente para involucrar a las partes en todos los ámbitos. Sin ella, una ENC tiende a resultar en una suma de actividades de agencias individuales según sus propias prioridades en lugar de un todo concertado, y conduce a una gestión de la ciberseguridad fragmentada, desigual y despilfarradora, agravando problemas similares en el futuro. El lanzamiento de una nueva ENC es un momento crítico para establecer su importancia nacional y garantizar una amplia participación de todas las partes interesadas. Un anuncio presidencial o del Primer Ministro, o al menos del ministro responsable de la estrategia, le dará mayor peso y conciencia.

Definir un buen modelo de gobernanza es uno de los elementos fundamentales para el éxito de una estrategia nacional de seguridad. El éxito de la gobernanza y la ejecución de las ENC puede lograrse tanto mediante un enfoque centralizado como descentralizado de la gobernanza, ambos con sus puntos fuertes y débiles. Mientras que la amplia autonomía de las organizaciones, característica del modelo de gobernanza descentralizada, estimula las alianzas creativas y la cooperación eficiente informal, la coherencia de las acciones y la asignación coordinada de recursos pueden ser más sencillas con el modelo de gobernanza de la ciberseguridad centralizada, mientras que la configuración de la gobernanza descentralizada debe considerar cuidadosamente el establecimiento de un entendimiento global sobre la división de responsabilidades, la coordinación, las responsabilidades y los mecanismos para la toma de decisiones.

Proporcionar una visión a largo plazo bien anclada y unos principios fundamentales es un poderoso medio para guiar el desarrollo estratégico basado en el valor que se mantiene coherente a lo largo de los periodos estratégicos, aunque está abierto a revisiones y ajustes cuando se justifique.

La Estrategia y su Plan de Acción son herramientas complementarias. En conjunto, garantizan coherencia y estabilidad al tiempo que se mantienen ágiles en un entorno en rápida evolución. La estrategia nacional de ciberseguridad establece una base común para los actores y las acciones, garantizando la coherencia entre los diversos objetivos y actividades, y proporcionando previsibilidad y estabilidad para todos los actores durante el periodo de la estrategia. El Plan de Acción, con su período de planificación centrado y su revisión periódica, debe garantizar la

agilidad y la capacidad de respuesta a la situación actual dentro de los límites de la estrategia. Para alcanzar los objetivos fijados en la ENC, cualquier política, legislación o estrategia sectorial posterior que aborde la ciberseguridad deberá ajustarse a la visión, los principios, los objetivos y los compromisos acordados en la ENC.

El sólido compromiso de las partes interesadas confiere calidad y legitimidad a la estrategia, pero debe ir acompañado de una responsabilidad mutua. A lo largo del proceso de la estrategia, se invita a las partes interesadas públicas y privadas a participar en el proceso de la estrategia, demostrando su ambición y contribuyendo con su experiencia a la creación de ciberresiliencia a nivel nacional. Sin embargo, la apropiación significa no sólo el derecho a expresar opiniones, sino también la participación en la asunción de responsabilidades. Pedimos a todos los implicados en el proceso estratégico que sigan tan comprometidos con la implementación de la estrategia como lo han estado con su desarrollo, y que se responsabilicen mutuamente de la obtención de resultados..

Un liderazgo comprometido es esencial para el éxito de la implementación de la estrategia nacional de ciberseguridad. El mantenimiento de una fuerte implicación y compromiso de las partes interesadas a través de un consejo de supervisión y asesoramiento es esencial para que la estrategia se lleve a cabo con éxito. Una estrategia nacional de ciberseguridad contribuye a la mejora continua de la ciberseguridad si se aplica; una estrategia que se queda en el cajón sin aplicar es un despilfarro de recursos y daña la confianza y la buena voluntad de las partes interesadas invertidas en el proceso. Una implementación comprometida a lo largo del tiempo también permitirá saber lo que funciona y lo que debe ajustarse, dónde podría aumentarse el nivel de ambición y dónde los objetivos podrían haber sido demasiado optimistas debido a complejidades imprevistas.

Por último, una ECN es un proceso con un ciclo de vida, más que un documento. La revisión periódica, el análisis y las lecciones aprendidas durante y al final del periodo de la estrategia deberían formar parte del enfoque estratégico para seguir desarrollando y reforzando la ciberseguridad nacional.

Herramientas y referencias

1. Catálogo de medidas de ciberseguridad (legales, técnicas, organizativas, desarrollo de capacidades, cooperación): (Catalog of national cybersecurity measures (legal, technical, organisational, capacity development, cooperation):

- International Telecommunication Union: Global Cybersecurity Index. https://www.itu.int/en/

ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

2. NCS lifecycle, principles and good practice:
    - Process and Guide to developing a National Cybersecurity Strategy. https://ncsguide.org/
3. Strategic, preventive and responsive capacity areas and indicators for national cybersecurity
    - e-Governance Academy: National Cybersecurity Index (NCSI). https://ncsi.ega.ee/ (12)
4. European Union elements of a national strategy
    - NIS 2016: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L1148
    - NIS2 for more advanced digital society

CYBER4Dev

www.cyber4dev.eu

Funded by the
European Union