INTERPOL

Guía sobre la Estrategia Nacional contra la Ciberdelincuencia

JAIF
Japan-ASEAN Cooperation

Abril de 2021

Prólogo

Conforme la tecnología de la información ha ido integrándose en nuestra sociedad, la ciberdelincuencia se ha convertido en un peligro común a escala mundial. Con más de 4 500 mil millones de personas en línea, la mitad de la población mundial está potencialmente en riesgo de ser víctima de la ciberdelincuencia.

La pandemia de COVID-19 ha tenido como consecuencia la aceleración de la fusión de nuestros espacios físico y cibernético, y ha aumentado la dependencia de la conectividad para muchas de nuestras tareas básicas tanto en el trabajo como en la vida personal.

Un panorama de la ciberdelincuencia cada vez más complejo, aunado a los desafíos inherentes de las investigaciones transfronterizas, ha supuesto una carga adicional para las fuerzas del orden de todo el mundo.

Mientras que el sector privado se ha ido transformando, el sector público continúa haciendo frente a los desafíos planteados por una falta de información, estrategias, recursos, infraestructuras y asociaciones.

Es importante que las fuerzas del orden reconozcan que las medidas, prácticas y políticas actuales no son suficientes para abordar una ciberdelincuencia en continua evolución, e identifiquen los pasos a dar para solucionar este déficit.

El sector público debe reforzar su nivel de preparación, eficacia y liderazgo para lograr la ciberresiliencia colectiva. La ciberseguridad es una responsabilidad compartida y un objetivo común hacia el que debemos trabajar continuamente.

Cuando se replican técnicas y tácticas en ataques a diferentes sectores por todo el mundo, se aprecia plenamente el verdadero valor de la plataforma mundial de INTERPOL para ayudar a los investigadores a intercambiar información de forma segura y a reaccionar con celeridad.

Como parte de los esfuerzos para apoyar a nuestros países miembros, me complace presentar la **Guía de INTERPOL sobre Estrategia Nacional contra la Ciberdelincuencia**.

El mundo está cada vez más conectado e INTERPOL continuará teniendo un papel único y central como parte de la comunidad mundial de las fuerzas del orden en nuestra lucha conjunta contra la ciberdelincuencia.

Jürgen Stock

Secretario General de INTERPOL

Introducción

Estamos en un nuevo paradigma en el que se fusionan los espacios físico y cibernético, y la transformación digital ha aumentado nuestra dependencia de la conectividad.

Las fuerzas del orden de todo el mundo han sido testigos directos de los aspectos delictivos específicos que la pandemia de COVID-19 estaba creando, especialmente la diversificación y el creciente impacto de la ciberdelincuencia. Este fenómeno nos ha hecho replantearnos nuestra respuesta y readaptar nuestra red mundial de las fuerzas del orden.

Un informe de INTERPOL de agosto de 2020, que estudiaba el impacto de la pandemia de coronavirus en el panorama mundial de las ciberamenazas, consideró que las estrategias nacionales de lucha contra la ciberdelincuencia eran una forma de crear resiliencia en las infraestructuras y servicios nacionales, ayudando a los países a hacer frente eficazmente a las ciberamenazas y proteger a las comunidades de los ciberataques durante la pandemia y después.

Con el mandato de «reducir el impacto global de la ciberdelincuencia y proteger a las comunidades para lograr un mundo más seguro», la Dirección de INTERPOL de Ciberdelincuencia ofrece capacidades policiales para luchar contra la ciberdelincuencia. Uno de sus principales objetivos es reforzar y mejorar las capacidades de los países miembros a fin de prevenir, detectar e investigar este tipo de delitos.

Esta Guía aporta a los países miembros de INTERPOL un valioso recurso para desarrollar o actualizar su Estrategia Nacional contra la Ciberdelincuencia. Ayuda a comprender mejor su respuesta actual ante este tipo de delitos, y proporciona los medios para diseñar una estrategia y un programa más robustos para superar los desafíos que están impidiendo dar una respuesta más efectiva a la delincuencia cibernética.

Recomiendo esta Guía a nuestros países miembros para hacer que sus países sean más resilientes y ágiles en este mundo altamente digitalizado y poder luchar eficazmente contra la ciberdelincuencia.

Craig Jones

Director de Ciberdelincuencia

Índice

Acrónimos

ASEAN - Asociación de Naciones del Asia Sudoriental

ACCDP - Proyecto de la ASEAN de desarrollo de capacidades para luchar contra la ciberdelincuencia

CERT - Equipo de Respuesta a Emergencias Informáticas

CSIRT - Equipo de Respuesta a Incidentes Cibernéticos

DDoS - Denegación de servicio distribuida

Europol - Agencia de la Unión Europea para la Cooperación Policial

TIC - Tecnologías de la Información y la Comunicación (TIC)

IoT - Internet de las Cosas

IP - Protocolo de Internet (PI)

ITU - Unión Internacional de Telecomunicaciones (UIT)

MLAT - Tratados de Asistencia Judicial Recíproca

SMART - *Specific, Measurable, Achievable, Relevant, y Time-Bound* (específicos, cuantificables, realizables, realistas, limitados en el tiempo)

UNODC - Oficina de las Naciones Unidas contra la Droga y el Delito (ONUDD)

Autores

Shane Cross, Simon Hirrle – INTERPOL

May-Ann Lim - TRPC Pte Ltd

Agradecimientos

La elaboración de esta Guía ha sido posible gracias al trabajo de muchas personas. Se realizaron consultas, talleres, revisiones por pares y reuniones. El Proyecto de la ASEAN de desarrollo de capacidades para luchar contra la ciberdelincuencia (ACCDP) quisiera agradecer su contribución a las siguientes personas implicadas en varias fases de la elaboración de esta Guía:

- Steve Honiss – Aardwolf Consulting Ltd
- Benjamin Ang - *S. Rajaratnam School of International Studies*, Universidad Tecnológica de Nanyang, Singapur
- Claire Pluckrose
- Anthony Teelucksingh - Ministerio de Justicia de los Estados Unidos
- Aysha Ahmed Bin Haji - Ministerio del Interior - Reino de Bahréin
- Jeannie Tsang *et al* – Servicios policiales de Hong Kong
- Dr. Cristos Velasco
- Yoichi Kumota - *National Center of Incident Readiness and Strategy for Cybersecurity*, Japón
- Ismamuradi Abdul Kadir – Ciberseguridad Malasia
- Representantes de países de la ASEAN en el taller de lanzamiento del ACCDP
- Dong Uk Kim, Pei Ling Lee, Wei Xian Tee - INTERPOL

Aviso legal

Esta Guía sobre la Estrategia Nacional contra la Ciberdelincuencia ("Guía") ofrece información y orientaciones generales para comprender y abordar la ciberdelincuencia desde una perspectiva estratégica, con el objetivo de desarrollar o mejorar una Estrategia Nacional contra la Ciberdelincuencia. La información en esta Guía se ha obtenido de los países miembros, asociados del sector privado y fuentes abiertas. Los conocimientos especializados y las orientaciones ofrecidas en esta Guía utilizan esta información, y se aportan para que el lector las considere siguiendo su propio criterio.

La intención de los ejemplos, descripciones y discusiones de esta Guía es ser opciones a considerar, más que recomendaciones, estímulos o propuestas definitivas. Cualquier acción, propuesta, medida o política desarrollada en base a lo expuesto, debe adoptarse de acuerdo con la legislación aplicable, algo que los lectores pertinentes deberán verificar y probar en las jurisdicciones correspondientes. INTERPOL no se responsabiliza de ninguna de esas acciones, pasos, medidas o de ningún documento creado basándose en esta Guía.

Los enlaces a publicaciones o sitios web externos incluidos en esta Guía se aportan únicamente como referencia, y no implican el respaldo de INTERPOL a dichas publicaciones o su contenido. Es responsabilidad del usuario evaluar el contenido y la utilidad de la información obtenida de esas publicaciones o sitios web.

Las descripciones de las disposiciones de ciertos instrumentos jurídicos en este documento se presentan solamente para su debate y no son, ni pueden interpretarse como, propuestas sobre interpretaciones aplicables en relación a cualquiera de estos instrumentos jurídicos.

El Modelo de Estrategia contra la Ciberdelincuencia incluido en la Guía se ofrece únicamente con fines educativos y como ejemplo o sugerencia para consideración del lector. No es vinculante en forma alguna ni tampoco está aprobado por INTERPOL como una estrategia efectiva. El lector podrá adoptarlo siguiendo su propio criterio, y deberá considerase teniendo en cuenta las políticas, leyes y circunstancias aplicables en el país en cuestión. INTERPOL no podrá ser tenido responsable de ningún daño o perjuicio resultado de su adopción en cualquier jurisdicción.

Aviso sobre derechos de autor

1. Introducción

Contexto

Esta Guía se ha elaborado como parte de la segunda fase del Proyecto de la ASEAN de desarrollo de capacidades para luchar contra la ciberdelincuencia (ACCDP II). El proyecto ACCDP está financiado por el Fondo de Integración Japón-ASEAN (JAIF) 2.0 a través de la Secretaría de ASEAN y con el Ministerio del Interior de Singapur como promotor del proyecto. INTERPOL es el organismo ejecutor.

El objetivo del proyecto es reforzar la capacidad de los países para luchar contra la ciberdelincuencia y trabajar juntos como región y a nivel internacional. El proyecto ACCDP aborda específicamente la necesidad de que las autoridades penales desarrollen sus conocimientos y habilidades en materia cibernética y creen asociaciones regionales mediante actividades y productos adaptados a la situación.

El proyecto ACCDP forma parte de la respuesta mundial de INTERPOL ante la ciberdelincuencia y apoya la implementación de su estrategia mundial contra la ciberdelincuencia. INTERPOL respalda las acciones nacionales de lucha contra la ciberdelincuencia, un tipo de delito que la Organización considera, junto al terrorismo y a la delincuencia organizada, como un área central a nivel mundial.

Metodología y enfoque en la elaboración de la Guía

Los resultados consolidados de las evaluaciones por país (Evaluación Nacional sobre la Ciberdelincuencia) realizadas en la primera fase del proyecto ACCDP revelaron una clara necesidad de disponer de una estrategia para combatir la ciberdelincuencia en muchos estados miembros de ASEAN (AMS). Por ello, se preparó esta Guía en la segunda fase del proyecto ACCDP.

La elaboración de la Guía comenzó con un taller de una semana de duración al que asistieron representantes de fuerzas del orden, organismos nacionales responsables de temas cibernéticos y asesores externos, y continuó con la aportación de varios especialistas de INTERPOL y sus países miembros.

La información contenida en esta Guía no está adaptada a ninguna región en concreto, sino que presenta buenas prácticas conocidas que se utilizan a nivel internacional.

Propósito de la Guía

La Guía está diseñada para ser utilizada por cualquier país que desee desarrollar, revisar o mejorar su Estrategia Nacional contra la Ciberdelincuencia.

El proyecto puso de manifiesto una disparidad significativa entre las iniciativas, legislaciones y procesos de lucha contra la ciberdelincuencia vigentes en los países miembros de INTERPOL, y subrayó la importancia de armonizarlas al máximo con las buenas prácticas internacionales.

Esta Guía se elaboró para aportar un enfoque metodológico a la potencialmente difícil tarea de crear o actualizar una estrategia de lucha contra la ciberdelincuencia.

2. Ciberdelincuencia y ciberseguridad

2.1 El reto de definir ciberdelincuencia

No existe una definición de ciberdelincuencia aceptada a nivel mundial. El enfoque más común es definir los términos claves utilizados en las investigaciones sobre ciberdelincuencia. Examinar definiciones utilizadas frecuentemente nos permitirá identificar conceptos claves y utilizar esas definiciones consistentemente en la estrategia de lucha contra la ciberdelincuencia de un país.

Un ejemplo de este enfoque es el *Model Law on Computer and Computer Related Crime* de 2017 de la Commonwealth («Ley Modelo de la Commonwealth»)[1]Esta ley comienza definiendo algunos términos claves: "datos informáticos", «medio de almacenamiento de datos informáticos», «proveedor de servicios», y «datos sobre el tráfico». Tras estas definiciones de términos claves, la Ley Modelo de la Commonwealth identifica los principales delitos que considera parte de la ciberdelincuencia – (1) acceso ilícito, (2) interferencia en los datos, (3) interferencia en los sistemas informáticos, (4) interceptación ilícita de datos, (5) dispositivos ilícitos y (6) utilización de niños en pornografía.

Este enfoque es muy similar al del Convenio sobre la Ciberdelincuencia del Consejo de Europa (Convenio de Budapest)[2], que contiene definiciones iniciales de «sistema informático», «datos informáticos», «proveedor de servicios», y «datos sobre el tráfico». El convenio define seguidamente cuatro categorías de delitos cometidos utilizando sistemas informáticos y tecnología de la información. Estas categorías son:

- Título 1: Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos –acceso ilícito, interceptación ilícita, interferencia en los datos, interferencia en el sistema y abuso de los dispositivos;
- Título 2: Delitos informáticos –falsificación informática, fraude informático;
- Título 3: Delitos relacionados con el contenido – utilización de niños en pornografía;
- Título 4: Delitos relacionados con el derecho de autor y los derechos afines;
- Título 5: Otras formas de responsabilidad y de sanciones –tentativa y complicidad, responsabilidad de las personas jurídicas.

Tabla 1: Comparación de términos claves sobre ciberdelincuencia

Término definido	Ley Modelo de la Commonwealth	Convenio de Budapest
Datos informáticos	Se entiende por «datos informáticos» toda representación de hechos, información o conceptos de un sistema informático, incluido un programa capaz de provocar que un sistema informático realice una función.	Por «datos informáticos» se entenderá cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función.
Medio de almacenamiento de datos informáticos	Se entiende por «medio de almacenamiento de datos informáticos» todo artículo o material (por ejemplo un disco) a partir del cual es posible reproducir información, con o sin ayuda de cualquier otro artículo o dispositivo.	(no define este término)
Sistema informático	Se entiende por «sistema informático» un aparato o grupo de aparatos interconectados o relacionados, incluida la Internet, en que uno o varios de ellos llevan a cabo, con arreglo a un programa, el procesamiento automático de datos o cualquier otra función.	Por «sistema informático» se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa.

[1] https://thecommonwealth.org/sites/default/files/key_reform_pdfs/P15370_11_ROL_Model_Law_Computer_Related_Crime.pdf

[2] https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

Término definido	Ley Modelo de la Commonwealth	Convenio de Budapest
Proveedor de servicios	Se entiende por «proveedor de servicios" (a) toda entidad pública o privada que ofrece a los usuarios de su servicio la capacidad de comunicar por medio de un sistema informático; y (b) cualquier otra entidad que procese o almacene datos informáticos en nombre de dicho servicio de comunicación o de los usuarios de dicho servicio.	Por «proveedor de servicios» se entenderá: (i) Toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar por medio de un sistema informático, y (ii) cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios de ese servicio.
Datos sobre el tráfico	Por «datos sobre el tráfico» se entiende los datos informáticos: (a) que se relacionan con una comunicación por medio de un sistema informático; (b) que son generados por un sistema informático que forma parte de una cadena de comunicación; y (c) que muestran cuáles son el origen, el destino, la ruta, la fecha y la hora, el volumen, la duración o el tipo de servicios subyacentes. .	Por «datos sobre el tráfico» se entenderá cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente..

La obtención de resultados positivos en investigaciones sobre ciberdelincuencia puede depender de la correcta recopilación, análisis y atribución de las pruebas digitales. El término «pruebas digitales» se utiliza indistintamente con pruebas electrónicas (e-evidence), y hace referencia a información y datos almacenados, recibidos o transmitidos por un dispositivo electrónico. Incluye pruebas procedentes de dispositivo digitales o registros obtenidos de proveedores de servicios en línea.

2.2 Delitos dependientes de medios electrónicos versus delitos facilitados por medios electrónicos

Además de definir los términos claves relacionados con la ciberdelincuencia –que puede ser un término amplio que abarca una multitud de delitos- es importante diferenciar entre «delitos dependientes de medios electrónicos», denominado también «ciberdelincuencia pura», y «delitos facilitados por medios electrónicos». La serie de documentos de investigación y análisis del Ministerio del Interior del Reino Unido titulada *Cybercrime: a review of the evidence*[3] ofrece una referencia útil y distingue ambos conceptos de la siguiente manera:

- «Delitos dependientes de medios electrónicos» (o delitos informáticos «puros») son delitos que solamente pueden cometerse utilizando un ordenador, redes informáticas u otra forma de tecnología de la información y la comunicación (TIC). Estos actos incluyen la propagación de virus u otro *malware*, piratería y ataques de denegación de servicio distribuida (DDoS). Son actividades dirigidas principalmente contra ordenadores o redes, aunque puede haber consecuencias secundarias. Por ejemplo, los datos recopilados pirateando una cuenta de correo electrónico pueden utilizarse ulteriormente para cometer un fraude[4].
- «Delitos facilitados por medios electrónicos» son delitos tradicionales, que pueden aumentar su volumen o alcance mediante el uso de ordenadores, redes informáticas u otras formas de TIC. Al contrario de los delitos dependientes de medios electrónicos, que dependen únicamente de las TIC, los delitos subyacentes de los delitos facilitados por medios electrónicos pueden cometerse sin el uso de estas tecnologías. Dos de los tipos más generalizados de delitos facilitados por medios electrónicos son fraude y robo[5]. Un ejemplo serían las estafas por correos electrónicos que intentan engañar al destinatario, incitándole a transferir dinero a un emisor desconocido.

3 https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence

4 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246751/horr75-chap1.pdf

5 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf

2.3 Ciberseguridad *versus* ciberdelincuencia

Si bien los términos «ciberseguridad» y «ciberdelincuencia» están interrelacionados y a menudo sus intereses se entrecruzan, los significados no son idénticos y el ámbito de lo que constituye «ciberseguridad» y «ciberdelincuencia» varía desde las perspectivas técnica, legal y política.

La siguiente tabla aclara el alcance de cada ámbito normativo:

Tabla 2: Definición de ciberseguridad y ciberdelincuencia

Ciberseguridad	**Ciberdelincuencia**
Definición	
Normalmente se define ciberseguridad como la protección de la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos a fin de mejorar la seguridad, la resiliencia, la fiabilidad y la confianza en las TIC. El concepto habitualmente abarca dimensiones políticas (intereses nacionales y seguridad), técnicas y administrativas.	La ciberdelincuencia se define como delitos cometidos contra datos informáticos, medios de almacenamiento de datos informáticos, sistemas informáticos o proveedores de servicios. El concepto habitualmente abarca categorías de delitos como acceso ilícito, interferencia en los datos y sistemas informáticos, fraude y falsificación, interceptación ilícita de datos, dispositivos ilícitos, explotación infantil e infracciones en materia de propiedad intelectual.
Enfoque reglamentario	
La regulación de la ciberseguridad se centra en la protección contra los ciberataques de las infraestructuras nacionales, así como del sector público y privado. Unas medidas sólidas de ciberseguridad protegen a los sistemas informáticos de acceso no autorizado, de ser dañados o de hacerlos inaccesibles. Busca reducir el riesgo de ciberataques y protege contra la explotación no autorizada de sistemas, redes y tecnologías mediante el uso de tecnologías, procesos y controles a nivel técnico, institucional o de procedimiento. La ciberseguridad se centra en la política y el procedimiento para asegurar y proteger sistemas y activos.	La regulación de la ciberdelincuencia se centra en establecer lo que el país considera como delitos dependientes de medios electrónicos y delitos facilitados por medios electrónicos, proporcionando al país instrumentos para criminalizar los delitos y autorizando la investigación y el enjuiciamiento de delitos de ciberdelincuencia. Las normativas sobre ciberdelincuencia se centran en el derecho sustantivo como el abuso de los dispositivos, derecho procesal como la conservación de los datos, y otras disposiciones como los tratados de Asistencia Judicial Recíproca y recolección de pruebas. Se establecen a fin de proteger a los ciudadanos mediante la identificación de los responsables de la comisión de delitos y el desmantelamiento de sus operaciones, levándolos ante la justicia como individuos o grupos de delincuencia organizada.
Cronología	
Las regulaciones relativas a la ciberseguridad normalmente están encaminadas a prevenir ataques *antes* de que se produzcan. La seguridad es un ciclo continuo que incluye la respuesta a incidentes y la revisión de los procesos que ocurren *después* de la detección de una infracción.	Las regulaciones relativas a la ciberdelincuencia normalmente definen y detectan actividades delictivas en el ciberespacio *después* de que ocurran, y aportan competencias a las fuerzas del orden para investigar las actividades *después* de que hayan ocurrido, con el fin de llevar a los delincuentes ante la justicia.

Una estrategia contra la ciberdelincuencia debe ir de la mano de una estrategia de ciberseguridad. En algunos incidentes cibernéticos, al principio puede no estar claro si se trata de un incidente de ciberseguridad que afecta a infraestructuras personales, de empresas o nacionales, o si es un incidente de ciberdelincuencia en el que se ha cometido un verdadero delito, o una combinación de ambos.

- En un incidente de ciberdelincuencia, se requeriría una respuesta de las fuerzas del orden y del sistema de justicia penal, por ejemplo, el organismo responsable de las investigaciones en materia de ciberdelincuencia.
- En un incidente de ciberseguridad, tendría que desplegarse el organismo o entidad pertinente responsable de la ciberseguridad, como un Equipo de Respuesta a Emergencias Informáticas (CERT) o un Equipo de Respuesta a Incidentes Cibernéticos (CSIRT).

El informe de 2017 de la Agencia de la Unión Europea para la Ciberseguridad (ENISA), *Tools and methodologies to support cooperation between CSIRTs and law"enforcement*[6] también confirmó que los CSIRT y las fuerzas del orden a menudo intercambian información durante la gestión e investigación de incidentes, tanto de manera formal como informal. Se citó la confianza como un factor clave del éxito para una cooperación efectiva. El informe resaltó que, a pesar de que los CSIRT y las fuerzas del orden tienen diferentes objetivos y métodos de recopilación y tratamiento de la información, hay una creciente comprensión recíproca entre las dos comunidades en cuanto a las necesidades[7].

Si un país todavía tiene que elaborar e implementar una estrategia de ciberseguridad, la guía *NCSS Good Practice Guide* de ENISA es un documento útil que puede ayudar en este proceso[8].

3. Factores que facilitan la ciberdelincuencia

Una serie de factores han contribuido a la creación de un entorno lucrativo para los ciberdelincuentes y de una enorme población de víctimas potenciales. Incluyen, pero no se limitan a:

3.1 Conectividad: más individuos en línea con un bajo nivel de sensibilización sobre seguridad digital

Hay un rápido aumento en el número de usuarios de internet, y una adopción directamente relacionada del uso de dispositivos móviles, comercio en línea, transacciones electrónicas y comunicaciones electrónicas. La poca sensibilización generalizada en materia de ciberseguridad y ciberhigiene, particularmente entre usuarios vulnerables como las personas mayores, **ha conducido a un drástico aumento en el número de víctimas de ciberdelincuencia.**

- Un estudio de 2018 realizado por una universidad estadounidense mostró que la inmensa mayoría de los usuarios particulares de internet tienen un bajo nivel de concienciación sobre ciberseguridad. Por ejemplo, no conocían la diferencia entre *software* antivirus y cortafuegos y tenían una ciberhigiene limitada (el 67 % de los participantes en la encuesta no tenían *software* antivirus actualizado, o, en algunos casos, ni siquiera lo tenían instalado. Muchos usuarios también comunicaban sin reservas sus contraseñas y compartían rápidamente información privada en las redes sociales[9].

3.2 Movilidad: negocios en línea con personal teletrabajando en redes menos seguras

Una mayor movilidad y un acceso más amplio a redes han conducido a un acusado incremento en el número de empleados que teletrabajan, inclusive desde sus casas. En consecuencia, hay más comunicaciones y transacciones comerciales y oficiales en redes y sistemas informáticos, públicos o privados, menos seguros (por ejemplo, personas trabajando desde cafeterías). **Esto ha aumentado la vulnerabilidad de las redes corporativas y, con ello, ha crecido la superficie de ataque para los ciberdelincuentes.**

---

6 https://www.enisa.europa.eu/publications/tools-and-methodologies-to-support-cooperation-between-csirts-and-law-enforcement

7 https://www.enisa.europa.eu/publications/csirts-le-cooperation/at_download/fullReport

8 https://www.enisa.europa.eu/publications/ncss-good-practice-guide/at_download/fullReport

9 https://par.nsf.gov/servlets/purl/10083310

- Un estudio publicado por INTERPOL en agosto de 2020 reveló que el *phishing*, las estafas y fraudes en línea y otras ciberamenazas habían aumentado en un 59 % tras la pandemia de COVID-19[10].
- Entre otras amenazas, el Foro Económico Mundial (WEF) informó en marzo de 2020 de la necesidad de que las empresas realizaran la transición para trabajar desde casa garantizando un método seguro para que los empleados se conecten a las aplicaciones fundamentales de la empresa. Asimismo, hay que garantizar la protección de las terminales en todos los dispositivos utilizados por los empleados para acceder a recursos del trabajo en línea, como la autenticación multifactor[11].

3.3 Interconectividad: ciudades y hogares en línea crean nuevas formas de vulnerabilidad

Smart Cities (ciudades inteligentes)
La mayor accesibilidad y miniaturización de los componentes de los ordenadores ha llevado a una aceleración en el despliegue de redes e infraestructuras *Smart City*. Ejemplos de estas redes de ciudades interconectadas son *ASEAN Smart Cities Network*[12] y *Smart Cities Mission* en India[13]. Si bien el desarrollo de las ciudades inteligentes es uno de los principales objetivos de muchas economías, también hace aumentar la **superficie de ataque potencial disponible para los ciberdelincuentes, que dirigen sus ataques a dispositivos inteligentes vulnerables.**

- En 2017, los ataques de *ransomware* como WannaCry y NotPetya pusieron de manifiesto los peligros que pueden plantear este tipo de ataques para las redes interconectadas, poniendo en riesgo a un gran número de dispositivos[14].

Smart Homes (hogares inteligentes)
Las ciudades inteligentes no son el único ejemplo de disponibilidad generalizada de dispositivos IoT. La creciente accesibilidad para los consumidores de dispositivos de hogares inteligentes amplía el número de dispositivos potencialmente vulnerables. Muchos usuarios de estos equipos no cambian las contraseñas predeterminadas ni actualizan regularmente el *software*, convirtiéndolos en blancos fáciles de ataque. Artículos comunes en los hogares, como cerraduras de puertas y refrigeradores, son ahora dispositivos con acceso a internet, proporcionando nuevas opciones de ataque para los ciberdelincuentes.

- En 2019, Kaspersky remarcó que, en los primeros seis meses del año, se detectaron más de 100 millones de ataques a dispositivos inteligentes. Supuso un drástico aumento en comparación con los 12 millones de ataques detectados el año anterior[15]. El informe afirma que los ciberdelincuentes prefieren dispositivos particulares antes que dispositivos corporativos[16] porque normalmente son blancos más fáciles.
- En 2020, las redes trampa de Kaspersky –redes de copias virtuales de varios dispositivos y aplicaciones conectados a internet– detectaron 426 millones de ataques en dispositivos IoT procedentes de 742 000 direcciones IP únicas solamente en los primeros seis meses del año. Implica que el número de ataques se ha cuadruplicado, y que hay 2,5 veces más números de IP comparado con el mismo periodo del año anterior.

---

10 https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19
11 https://www.weforum.org/agenda/2020/03/covid-19-cyberattacks-working-from-home/
12 https://asean.org/asean/asean-smart-cities-network/
13 http://smartcities.gov.in/content/innerpage/strategy.php
14 https://www.wsj.com/articles/how-hackers-could-break-into-the-smart-city-11568776732
15 https://www.kaspersky.com/about/press-releases/2019_iot-under-fire-kaspersky-detects-more-than-100-million-attacks-on-smart-devices-in-h1-2019
16 https://securelist.com/iot-a-malware-story/94451/

3.4 Sofisticación: responsables de amenazas con habilidades y tácticas en evolución

Los responsables de las amenazas cometen actos de ciberdelincuencia por diferentes motivaciones, entre ellos:

- activistas hackers que utilizan internet como medio de protesta;
- delincuentes como:
  - principiantes oportunistas o curiosos poniendo a prueba sus habilidades,
  - autores de delitos contra menores en línea,
  - grupos de delincuencia organizada dispuestos a ganar dinero;
- grupos de amenaza avanzada persistente promovidos por un estado-nación (APT) que llevan a cabo actividades de espionaje, recaudación de fondos o ataques a infraestructuras fundamentales.

Figura 1: Espectro de las ciberamenazas

Fuente desconocida

En los últimos años se ha visto la evolución de la ciberdelincuencia como servicio, por la que la ciberdelincuencia adquiere carácter de empresa comercial, poniendo sus servicios al alcance de todo aquel dispuesto a pagar. Dichas transacciones normalmente tienen lugar en la web oscura, la parte oculta de internet solamente accesible con navegadores especiales. Los ciberdelincuentes aprovechan el anonimato de los mercados y foros de discusión de la web oscura para ampliar sus habilidades y herramientas.

Un ejemplo de ciberdelincuencia como servicio es el *malware* Satan, que pertenece a la familia de *ransomware* Gen: Trojan.Heur2.FU. El *malware* Satan se puso a disposición del público a través de una plataforma *ransomware* como servicio (RaaS)[17].

Cada vez son más comunes las operaciones de *ransomware* a gran escala que causan perturbación y destrucción generalizada a infraestructuras personales, corporativas y nacionales. Ejemplos de ello son:

- En 2020, la empresa de fitness y dispositivos Garmin fue atacada con el *ransomware* WastedLocker. Supuestamente, la empresa pagó un rescate de 10 millones USD a los delincuentes para recuperar sus sistemas y evitar que salieran a la luz los datos de los usuarios[18] ;

17 https://www.zdnet.com/article/satan-ransomware-as-a-service-starts-trading-in-the-dark-web/
18 https://www.wired.com/story/garmin-ransomware-hack-warning/

- En octubre de 2020, la CISA (*Cybersecurity & Infrastructure Security Agency*) de los Estados Unidos emitió una alerta sobre el aumento de actividad de *ransomware* dirigida al sector sanitario y de la salud pública[19].

3.5 Falta de información: reticencia a informar sobre delitos de ciberdelincuencia

En muchos casos, las empresas y los particulares, víctimas de ciberdelincuencia, no denuncian el incidente a las autoridades. **Esto causa una falta de datos sobre cómo operan los ciberdelincuentes y sobre las tecnologías utilizadas para cometer delitos.** Desafortunadamente, es algo muy extendido[20].

- Las víctimas particulares a menudo no saben cómo ni dónde denunciar casos de ciberdelincuencia, creen que no merece la pena denunciarlo o se avergüenzan de haber sido víctimas de una estafa[21]. En muchos casos, el incidente no tiene como consecuencia la pérdida de vidas o bienes materiales (como datos o información personales) y, por ello, las víctimas no son conscientes o no están seguras de ser víctimas de un delito, por lo que no lo denuncian a las autoridades.
- Las empresas afectadas a menudo son reticentes a denunciar casos de ciberdelincuencia, pues hacerlo público puede ser negativo para el negocio y podría erosionar la confianza en la empresa de inversores y del mercado[22]. En muchos países, se está abordando esta cuestión mediante normas de protección de datos que obligan a denunciar ciberincidentes.
- En algunos casos, las víctimas de ciberdelincuencia pueden encontrar el proceso de denuncia complejo y poco claro, algo que les disuade de informar sobre incidentes.

3.6 Legislación y jurisdicción: falta de criminalización de la ciberdelincuencia y complejidad interjurisdiccional

La ciberdelincuencia implica frecuentemente investigaciones transfronterizas, pues las víctimas, los delincuentes y las infraestructuras pueden estar en diferentes países. Esto plantea un reto para los investigadores al constatar que otros países pueden no tener las mismas leyes que criminalizan el delito, se requieran distintos elementos para probar que ha ocurrido el delito o haya diversos periodos de conservación de datos de abonados. En algunos países, incluso puede haber una falta de legislación y, en consecuencia, de criminalización de la ciberdelincuencia, lo que crea una situación en la que el país se convierte en un refugio seguro para los ciberdelincuentes.

Además, es importante que los marcos jurídicos de los países otorguen el tiempo adecuado para la recopilación, análisis y divulgación de las pruebas digitales. Los plazos demasiado cortos pueden impedir obtener pruebas fundamentales, analizarlas debidamente o ser admitidas a tiempo, y, en consecuencia, los ciberdelincuentes no son enjuiciados.

Realizar investigaciones eficaces en las que haya implicadas múltiples jurisdicciones también incluye el establecimiento de asociaciones con homólogos de otros países a fin de hacer avanzar la investigación. Puede implicar llevar a cabo registros e incautaciones de pruebas físicas y/o digitales, o proporcionar autorizaciones judiciales como órdenes judiciales a entidades del sector privado, por ejemplo, empresas de telecomunicaciones y proveedores de internet.

Estas son solamente algunas de las dificultades de realizar investigaciones interjurisdiccionales eficaces con el fin de enjuiciar exitosamente casos de ciberdelincuencia.

---

19 https://us-cert.cisa.gov/ncas/alerts/aa20-302a
20 https://www.zdnet.com/article/cyber-crime-under-reporting-of-attacks-gives-hackers-a-green-light-say-police/
21 https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/reporting-cybercrime.html
22 https://www.infosecurity-magazine.com/opinions/organizations-failing-report/

4. Metodología: Desarrollo de una estrategia contra la ciberdelincuencia

La tarea inicial de desarrollo de una estrategia contra la ciberdelincuencia puede parecer abrumadora. Contar con un proceso de elaboración en el que basarse ayudará a elaborar la estrategia.

Existen numerosos modelos para la elaboración de políticas y, en general, se requieren los siguientes procesos:

Figura 2: Ciclo de vida de la estrategia

Fuente: TRPC, 2020

4.1 Sentar las bases de la estrategia

Antes de comenzar a desarrollar una estrategia contra la ciberdelincuencia, es importante comprender por qué lo está haciendo.

La ciberdelincuencia es una de las formas de delincuencia transnacional en más rápida expansión a la que se enfrentan los países miembros de INTERPOL. Si bien la veloz evolución de las TIC ha permitido el crecimiento económico y social, una creciente dependencia de internet ha creado más riesgos y vulnerabilidades, así como nuevas posibilidades para las actividades delictivas.

La ausencia de fronteras en la ciberdelincuencia implica que las fuerzas del orden se enfrentan al reto de responder eficazmente teniendo en cuenta las limitaciones de las investigaciones transfronterizas, los desafíos en materia jurídica y la diversidad de capacidades por todo el mundo.

A fin de hacer frente a estos desafíos y proteger a sus ciudadanos de la ciberdelincuencia, los países necesitan una estrategia clara.

Son numerosas las razones y ventajas de desarrollar una estrategia contra la ciberdelincuencia, tal como veremos en las siguientes secciones.

4.1.1 La ciberdelincuencia destruye la economía

En el ciberataque mundial NotPetya de junio de 2017, un *ransomware* afectó a operadores logísticos mundiales y a sus clientes. Cambios de ruta de última hora, compensaciones y mantener la cadena de suministros mundial costó a Maersk hasta 300 millones USD[23]. El daño no se limitó a su empresa, pues sus clientes se vieron también seriamente afectados por el incidente. Entre otros, la empresa de suministros médicos Merck perdió 870 millones USD; FedEx's TNT Express perdió 400 millones USD y la empresa de chocolates Cadbury perdió 188 millones USD.

Este efecto dominó de la ciberdelincuencia se puso igualmente de manifiesto cuando un ataque DDoS a gran escala utilizando el *botnet* Mirai se lanzó contra el proveedor de nombres de dominio Dyn en 2016, paralizando los negocios de muchos de los 178 000 clientes que tenían sus dominios de internet alojados en la empresa[24]. Estos incidentes resaltan la creciente sofisticación y transmisibilidad de los nuevos métodos de la ciberdelincuencia, que han evolucionado de generaciones anteriores de incidentes de ciberdelincuencia como Stuxnet, un virus informático que infectó al menos cuatro compañías de petróleo y gas: Baker Hughes, ConocoPhillips, Marathon y Chevron[25].

El informe sobre riesgos mundiales del año 2020 del Foro Económico Mundial estima que el coste de los daños causados por la ciberdelincuencia podría alcanzar 6 billones USD en 2021[26].

Una estrategia contra la ciberdelincuencia define los pasos necesarios para establecer una buena gobernanza de los datos en la empresa y una correcta ciberhigiene personal a fin de limitar el efecto económico.

4.1.2 La ciberdelincuencia facilita la comisión de otros delitos

Según la Oficina de las Naciones Unidas contra la Droga y el Delito (ONUDD), los incidentes de ciberdelincuencia a menudo están organizados por redes delictivas que operan en línea y que utilizan las ganancias obtenidas de los rescates y otras ganancias ilícitas para financiar otros delitos graves y el terrorismo[27].

Una estrategia contra la ciberdelincuencia sirve de apoyo a la lucha contra el terrorismo y contra el blanqueo de capitales, y limita los mecanismos de financiación de las redes de delincuencia organizada.

4.1.3 La ciberdelincuencia debilita las funciones de los gobiernos y puede costar vidas

Los ciberataques de *ransomware* causan estragos en todos los sectores. En muchos casos, se ven afectados servicios esenciales como hospitales y organismos de atención sanitaria, donde la inutilización de los sistemas informáticos puede causar la pérdida de vidas. Por ejemplo, en 2017, el ataque de *ransomware* WannaCry afectó al sistema sanitario del Reino Unido (NHS), dejando fuera de servicio los sistemas médicos, en algunos casos mientras los doctores estaban realizando operaciones críticas como intervenciones cardíacas[28].

---

23 https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
24 https://www.corero.com/blog/financial-impact-of-mirai-ddos-attack-on-dyn-revealed-in-new-data/
25 https://isssource.com/stuxnet-hit-4-oil-companies/
26 http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf
27 https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime-activities.html
28 https://www.dailymail.co.uk/news/article-4503420/It-s-life-death-NHS-patients-say-cyber-attack.html

De la misma manera, en septiembre de 2020, un hospital en Düsseldorf (Alemania) sufrió un ataque de *ransomware*. Al estar los sistemas del hospital bloqueados, una paciente con un problema que ponía en riesgo su vida tuvo que ser trasladada a otro hospital donde falleció por el retraso en recibir asistencia[29].

Una estrategia contra la ciberdelincuencia debe funcionar de forma conjunta con una estrategia de ciberseguridad para garantizar que no se perturben los servicios críticos.

4.1.4 Ventajas de elaborar una estrategia

Además de otras ventajas, una estrategia:

- Informa a todos los que pueden contribuir positivamente y beneficiarse;
- Ayuda a comprender mejor las vulnerabilidades del país;
- Muestra los avances para abordar los desafíos planteados por la ciberdelincuencia;
- Proporciona un marco establecido de prevención, detección y respuesta;
- Crea conciencia.

4.1.5 Requisitos de una estrategia

4.1.5.1 Establecer la autoridad del proyecto

Desarrollar una Estrategia Nacional contra la Ciberdelincuencia requiere la cooperación de muchas partes interesadas. Un reto común a la hora de establecer una estrategia contra la ciberdelincuencia es garantizar y mantener el compromiso de las partes pertinentes.

Por ello, es importante identificar una «autoridad del proyecto» formada por un funcionario de alto nivel, idealmente un ministro, y un equipo de proyecto con la responsabilidad de desarrollar, implementar y revisar la estrategia contra la ciberdelincuencia.

El funcionario de alto nivel es propietario del documento y debe garantizar que:

- el equipo de proyecto cuente con la cooperación necesaria de todas las partes interesadas claves;
- haya suficientes recursos disponibles para poner en práctica la estrategia.

Por ejemplo, el funcionario de alto nivel podría ser el Ministro del Interior y el equipo de proyecto podría estar formado por miembros de la unidad nacional de ciberdelincuencia. Alternativamente, el equipo de proyecto podría ser un grupo especializado conjunto.

La autoridad del proyecto también forma parte del comité rector (ver sección 4.2.1).

➔ Contar con el líder apropiado y un equipo de proyecto es esencial para lograr una estrategia contra la ciberdelincuencia fructuosa.

4.1.5.2 Obtener cooperación intragubernamental

Para que la elaboración de una estrategia sea eficaz, debe haber cooperación intrainstitucional. Puede ser una tarea difícil y requerir buenas dotes de liderazgo, colaboración efectiva y, a menudo, compromiso. Una cooperación intrainstitucional eficaz es fundamental en todas las etapas del proyecto, como la elaboración y la implementación de la estrategia contra la ciberdelincuencia.

La autoridad del proyecto debe consultar a los organismos socios pertinentes para obtener sus contribuciones y apoyo.

---

29 https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html

Una vez obtenido el acuerdo sobre el concepto del proyecto, se recomienda que la autoridad del proyecto establezca un mecanismo para garantizar la cooperación intragubernamental. Este mecanismo de cooperación puede incluir reuniones periódicas de todas las partes interesadas pertinentes, por ejemplo, como parte de un comité rector (ver sección 4.2.1).

➔ Asegúrese de contar con la participación de organismos socios antes de comenzar el proyecto.

4.1.5.3 Conseguir suficiente presupuesto y recursos

No es raro que los organismos gubernamentales tengan limitaciones financieras y de recursos. Esto puede afectar a la capacidad para realizar el proyecto e implementar una Estrategia Nacional contra la Ciberdelincuencia.

Para que el proyecto tenga éxito, es esencial planificar y asignar los recursos específicos apropiados. Se incluye aquí capital (presupuesto dedicado) y personal (personal dedicado al proyecto).

De la misma forma, se requiere una asignación adecuada de recursos humanos y financieros para la implementación de la estrategia contra la ciberdelincuencia (ver sección 4.4.).

➔ Asegúrese de contar con recursos suficientes ante de comenzar el proyecto.

4.1.5.4 Establecer objetivos SMART

Figura 3: Objetivos SMART

El ciclo de vida de la estrategia contra la ciberdelincuencia debe seguir los principios de los objetivos SMART[30]: deben ser específicos, cuantificables, realizables, relevantes y limitados en el tiempo. Por tanto, el proyecto debe comenzar estableciendo objetivos específicos a alcanzar en un plazo determinado, incluyendo indicadores cuantificables y fechas de entrega.

Un ejemplo sería identificar las partes interesadas pertinentes de las distintas etapas del ciclo de vida de la estrategia contra la ciberdelincuencia en un plazo de seis semanas.

➔ Considere adoptar este enfoque para aclarar las ideas, enfocar los esfuerzos, utilizar su tiempo y recursos de forma productiva, y finalmente, aumentar la posibilidad de que su proyecto y la estrategia contra la ciberdelincuencia tengan éxito.

4.2 Formulación de la estrategia

En este proceso se diseña y redacta la estrategia contra la ciberdelincuencia por los motivos y beneficios establecidos en el punto 4.1.

4.2.1 Designación del comité rector e identificación de las partes interesadas claves

Algunos estudios muestran que, frecuentemente, el éxito de las políticas públicas depende en gran medida del compromiso y la gestión de las partes interesadas[31]. Las estrategias que no logran obtener el compromiso, el apoyo o la implicación de las partes interesadas suelen estar faltos de recursos y atención, y no son prioritarios.

---

30 https://www.achieveit.com/resources/blog/the-history-and-evolution-of-smart-goals
31 http://www.oecd.org/gov/regulatory-policy/BPPs-for-Public-Consultation.docx

En una primera fase, es útil crear un comité rector formado por la autoridad del proyecto y otros funcionarios relevantes de alto nivel que deben elegirse en base a su capacidad de aportar supervisión estratégica y orientaciones en las distintas fases del ciclo de vida de la estrategia contra la ciberdelincuencia.

El comité rector debe determinar qué partes interesadas deben estar implicadas en la formulación de la estrategia contra la ciberdelincuencia. Estas partes interesadas consultadas ("los asesores") normalmente procederán de organismos gubernamentales y entidades no gubernamentales.

Organismos gubernamentales:

- La Unidad Nacional contra la Ciberdelincuencia, para intercambiar experiencias y conocimientos sobre investigación de la ciberdelincuencia;
- El principal organismo de ciberseguridad, con el fin de intercambiar experiencias sobre respuesta a ciberincidentes y redactar políticas de ciberseguridad, inclusive estrategias;
- Otras fuerzas del orden, con el objetivo de ayudar a comprender cuestiones y procesos de carácter regional en la investigación de la ciberdelincuencia, como la recolección de pruebas digitales;
- Funcionario(s) de alto nivel relevante(s) de los ministerios pertinentes, particularmente aquellos que puedan prestar autoridad y apoyo a la redacción o adopción de la estrategia contra la ciberdelincuencia. Entre ellos, funcionarios del Ministerio del Interior y del Ministerio de Derecho o Justicia, por ejemplo;
- Funcionarios fiscales y judiciales pertinentes, para asesorar sobre la aplicación de las leyes sobre ciberdelincuencia en el país;
- Otros funcionarios y equipos gubernamentales relevantes, como los procedentes de oficinas responsables de investigar fraudes, o funcionarios de ministerios relacionados con las TIC, la seguridad pública, etc.

Entidades no gubernamentales:

- Académicos/grupos de reflexión capaces de aportar conocimientos sobre temas actuales, y ofrecer habilidades de investigación y redacción;
- Órganos relacionados con la tecnología y la industria que mejor puedan identificar las amenazas más importantes a las que se enfrentan los negocios;
- Grupos de la sociedad civil, para que ayuden en labores de sensibilización;
- Órganos regionales e internacionales para intercambiar perspectivas sobre amenazas regionales de la ciberdelincuencia.

Elegir a los asesores adecuados cubrirá todo el abanico de necesidades de las partes interesadas y proporcionará unos buenos cimientos para la redacción de la estrategia contra la ciberdelincuencia. Cualquier parte interesada que no sea consultada en las primeras etapas, pero se incorpore más adelante, puede perturbar e incluso socavar todos los esfuerzos anteriores.

Tras la identificación de los asesores, se selecciona entonces un grupo más reducido con las personas mejor capacitadas para la redacción ("los redactores") para la ulterior elaboración de la estrategia (ver sección 4.2.3 Producción).

4.2.2 Balance, evaluación y análisis

Es esencial que los países examinen los procesos, recursos y habilidades disponibles para luchar contra la ciberdelincuencia. Este ejercicio también aportará valiosas perspectivas sobre áreas en las que hay deficiencias. Como resultado, el país tendrá una idea más clara de su panorama actual en materia de ciberdelincuencia y podrá comenzar a trabajar para construir el futuro que desea, reforzando su capacidad global para combatir la ciberdelincuencia.

La auditoría para hacer balance debe tener en cuenta las siguientes categorías:

4.2.2.1 *Personal y equipos*

Esta auditoría evalúa los recursos humanos disponibles o que trabajan en una función relacionada con la ciberdelincuencia, por ejemplo, personal especializado en ciencias forenses digitales y ciberdelincuencia o personal de ciberseguridad como los CERT.

Algunos ejemplos de organismos que podrían incluirse aquí son:

- Policía Nacional – departamentos y unidades
- Agencia o Departamento Nacional para la Ciberseguridad (si existiese)
    - Equipo Nacional de Respuesta a Incidentes Cibernéticos (CSIRT) y/o CERT
- Ministerio de derecho o justicia nacional, regional y estatal/provincial
    - jueces especializados en ciberdelincuencia
    - fiscales especializados en ciberdelincuencia
    - servicios de investigación
- Autoridad central encargada de la gestión de los Tratados de Asistencia Judicial Recíproca (MLAT)
- Agencia nacional de seguridad o inteligencia
- Otros organismos nacionales encargados de los delitos facilitados por medios electrónicos (por ejemplo, fraude, explotación, etc.)
- Otros servicios policiales a nivel de estado o provincia con unidades de investigación en materia de ciberdelincuencia.

Cada uno de estos organismos debe aportar un informe que incluya lo siguiente:

- Un resumen sobre su organismo, y la estructura organizativa y mandato de las unidades relevantes;
- Explicación de los tipos de ciberdelincuencia que abarcan;
- El marco jurídico en el que operan;
- Iniciativas en curso contra la ciberdelincuencia por cualquiera de los organismos.

Considere también las capacidades tecnológicas de los distintos organismos. ¿Cuentan con los equipos adecuados y la formación apropiada para llevar a cabo esta tarea?

4.2.2.2 *Proceso: Evaluación del entorno legislativo y regulador*

Evalúa los mecanismos legislativos y reguladores existentes en el país que tratan sobre la ciberdelincuencia. Incluye toda la legislación relevante, acuerdos de cooperación internacionales, normas y procedimientos operativos internos, costumbres y prácticas locales, etc.

Los aspectos de procedimiento pueden incluirse en las siguientes categorías:

- **Legislación sustantiva** como leyes sobre protección de datos personales o privacidad de datos; leyes que penalizan delitos como piratería y robo de datos; leyes que penalizan la venta de herramientas o servicios para la piratería; leyes contra el acoso en línea; y leyes que describen los requisitos para proteger las infraestructuras fundamentales.
- **Legislación procesal** como leyes sobre la recopilación y uso de pruebas electrónicas; normas sobre registro e incautación de pruebas electrónicas; normas sobre supervisión electrónica.
- **Acuerdos de cooperación internacionales** como los MLAT, adhesión al Convenio de Budapest[32], uso activo de la afiliación a INTERPOL para acceder a sistemas de cooperación internacional.

Los asesores pueden revisar legislación existente e identificar lagunas en el marco jurídico del país. En algunos casos, puede ser necesario unificar un número de legislaciones diferentes. Podría también

[32] https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

requerirse la actualización de leyes para criminalizar adecuadamente la ciberdelincuencia y la actualización de normativas que regularizan y posibilitan el registro, incautación y admisibilidad de pruebas electrónicas en investigaciones judiciales. Además de la legislación sobre ciberdelincuencia, pueden requerir revisión los poderes de investigación de las fuerzas del orden, cuestiones jurisdiccionales, la protección de datos, la privacidad y el derecho mercantil en relación a la confiscación de los beneficios de la ciberdelincuencia.

4.2.2.3 Autoevaluación y análisis

Una vez concluida la auditoría para hacer balance, debe llevarse a cabo una evaluación para identificar vulnerabilidades y áreas de mejora. Existen varias herramientas disponibles para realizar evaluaciones nacionales y cuantificar la capacidad cibernética del país.

La Unión Internacional de Telecomunicaciones (ITU) realiza una evaluación global periódica por país en materia cibernética. ITU controla y compara los compromisos de ciberseguridad de los países examinando cinco pilares: jurídico, técnico, organizativo, capacitación y cooperación. También considera los resultados de otras herramientas de evaluación existentes como el *Capability Maturity Model* (CMM) y el *Cyber Readiness Index* del Instituto Potomac. El producto resultante es el índice mundial de ciberseguridad (*Global Cybersecurity Index*, GCI)[33].

Una minuciosa herramienta de autoevaluación es la herramienta de 2017 del Banco Mundial *Combatting Cybercrime Evaluation Tool and Toolkit*. Este recurso[34] cuenta con una herramienta de evaluación[35], que es un fichero Excel automatizado que permite al usuario determinar lagunas en su capacidad actual para combatir la ciberdelincuencia y pone de manifiesto áreas a las que dirigir los recursos. Le acompaña una guía (*Toolkit*[36]) que aporta el contexto de la herramienta de evaluación. El primer uso de esta herramienta ofrece una base que puede controlarse periódicamente. Ambas herramientas (*Evaluation Tool y Toolkit*) deben utilizarse simultáneamente.

El índice mundial de ciberseguridad de la ITU normalmente se publica una vez al año, aunque los países pueden realizar una autoevaluación utilizando las herramientas del Banco Mundial a su conveniencia.

Los resultados de la evaluación que realiza el país pondrán de relieve vulnerabilidades y áreas de mejora. Estas deben considerarse como áreas de interés para la estrategia, tal como se considerará en la próxima sección.

Dependiendo de la herramienta de evaluación que utilice y su resultado, puede ser beneficioso estructurar los resultados utilizando métodos de análisis de probada eficacia como:

- Análisis DAFO (SWOT) – debilidades, amenazas, fortalezas, oportunidades
- Análisis PESTLE – político, económico, social, tecnológico, legal y medioambiental

El método elegido debe permitir a los responsables políticos determinar cuáles de las lagunas identificadas en la autoevaluación deben tener prioridad para actuar de inmediato, a medio plazo o a largo plazo.

---

33 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
34 https://www.combattingcybercrime.org/
35 https://www.combattingcybercrime.org/#assessment
36 https://www.combattingcybercrime.org/#toolkit

4.2.2.4 *Áreas de interés, objetivos estratégicos y medidas*

Figura 4: Áreas de interés, objetivos estratégicos y medidas

A partir de su autoevaluación y análisis (sección 4.2.2.3), los países identifican las áreas de interés que desean abordar como, por ejemplo, el marco jurídico. Se definen entonces los objetivos estratégicos para esa área de interés. Por ejemplo, «desarrollar un marco jurídico más eficaz para investigar y enjuiciar la ciberdelincuencia». Esto dará lugar a una o más medidas que serán completadas por los «propietarios de la medida», por ejemplo, actualizar leyes existentes en materia de ciberdelincuencia y redactar nuevas leyes.

Áreas de interés –aquellas áreas que el país intenta mejorar- son las piezas angulares de la estrategia que define el país basándose en los resultados de la autoevaluación y el análisis. Es el primer paso para la creación de la estructura que garantice que el país estará más capacitado para combatir la ciberdelincuencia.

Las áreas de interés son los temas generales de la estrategia y tienen una mayor duración que los objetivos estratégicos y las medidas.

Los objetivos estratégicos son declaraciones claramente definidas de los resultados a los que aspira llegar un país en un periodo de tiempo determinado.

Las medidas están definidas por la autoridad del proyecto y las partes interesadas pertinentes (sección 4.2.1, "asesores") basándose en su idoneidad para ayudar a lograr los objetivos estratégicos. Las medidas deben seguir el modelo SMART (sección 4.1.5) y deben intentar dar una respuesta a las siguientes preguntas:

- ¿Cómo puede alcanzarse el objetivo estratégico?
- ¿Existen programas o mecanismos que aborden el objetivo estratégico?
- ¿Cómo pueden mejorarse los programas o mecanismos existentes?
- ¿Qué nuevos programas o mecanismos deben crearse o desarrollarse?
- ¿Cómo se ejecutarán?
- ¿En qué periodo de tiempo?
- ¿Cómo se medirá el éxito (indicadores de éxito)?

Una vez las áreas de interés, los objetivos estratégicos y las medidas estén claramente establecidos, pueden resumirse en una sencilla tabla de referencia, como la que se muestra seguidamente:

Tabla 3: Ejemplo de tabla resumen de las áreas de interés, los objetivos estratégicos y las medidas

Áreas de interés	Objetivos estratégicos	Medidas
Marco jurídico	Desarrollar un marco jurídico más eficaz para investigar y enjuiciar la ciberdelincuencia.	• Redactar e implementar leyes pertinentes sobre ciberdelincuencia en un plazo de 18 meses (organismo ejecutor: Ministerio de Derecho). • Garantizar la adhesión al Convenio de Budapest sobre la ciberdelincuencia dentro de un plazo de dos años (organismo ejecutor: Grupo especializado conjunto entre Ministerio de Derecho y Ministerio de Asuntos Exteriores).
Capacitación	Garantizar la capacitación de los funcionarios públicos, en particular las autoridades fiscales, judiciales y las fuerzas del orden.	• Desarrollar y establecer un plan de estudio y formación sobre ciberdelincuencia para las autoridades encargadas de la aplicación de la ley, para comenzar en un plazo de 12 meses (organismo ejecutor: Ministerio del Interior/ Ministerio de Seguridad Pública o similar). • Desarrollar y establecer formación sobre fundamentos de las pruebas digitales para jueces y fiscales, para comenzar en un plazo de 12 meses (organismo ejecutor: Oficina del Fiscal General, Ministerio de Derecho/Ministerio de Justicia)
Asociaciones	Promover acuerdos y asociaciones para el intercambio de información a nivel nacional e internacional.	• Crear acuerdos de intercambio público-privados sobre inteligencia cibernética en un plazo de ocho meses (organismo ejecutor: Departamento de Ciberdelincuencia de la Policía). • Establecer un sistema de alerta de ciberamenazas en un plazo de nueve meses entre el sector público y privado, dando prioridad a sectores fundamentales (organismo ejecutor: Grupo especializado conjunto entre el Departamento de Ciberdelincuencia y el Ministerio de Comercio e Industria, colaborando con otros ministerios pertinentes).

4.2.3 Producción

La producción de la estrategia contra la ciberdelincuencia es la etapa del ciclo de vida de la estrategia que probablemente lleve más tiempo. A fin de ayudar en su redacción, esta Guía ofrece a los países un modelo a seguir (Capítulo 5).

4.2.3.1 Consulta a las partes interesadas

Debe emprenderse un proceso iterativo proponiendo áreas de interés para su debate con las partes interesadas ("asesores"). De esta manera, las partes contribuyentes tienen la oportunidad de aportar sus ideas sobre cómo progresar en las áreas de interés, dando forma así a los objetivos estratégicos (ver sección 5.4).

4.2.3.2 Primer proyecto de la estrategia contra la ciberdelincuencia

Este es el momento en el que el grupo de redactores nombrado previamente (sección 4.2.1) crea un primer proyecto de la estrategia contra la ciberdelincuencia teniendo presente las razones y las ventajas descritas en la sección 4.1 y los resultados del balance descrito en la sección 4.2.2.

Es habitual que el proyecto de estrategia pase por una serie de fases de escritura, consulta, comentarios, revisión y modificación. Cuanto más concienzudamente se realicen estas fases, más probabilidades habrá de que la estrategia final alcance el consenso entre las partes interesadas.

Los redactores pueden remitirse al Modelo de Estrategia contra la Ciberdelincuencia (Capítulo 5) donde se propone una estructura del documento.

4.3 Adopción de la estrategia

Una vez finalizado el proceso de formulación de la estrategia, un proyecto final de la estrategia contra la ciberdelincuencia estará listo para ser presentado formalmente para su adopción e implementación.

Este proceso variará entre países. Algunos requerirán que se debata la estrategia en una asamblea nacional, parlamento o algún otro foro de políticas público antes de ser presentada para su aprobación, por ejemplo, ser aprobada en el Parlamento/Congreso Nacional/Asamblea, o ser presentada al Jefe de Gobierno/Estado para su visto bueno.

4.4 Implementación de la estrategia

A fin de que la estrategia contra la ciberdelincuencia tenga éxito, debe haber un enfoque estructurado de la implementación. La implementación variará de un país a otro, aunque por lo general seguirá los siguientes pasos:

- Determinación de los pormenores sobre cómo se alcanzarán los objetivos estratégicos (sección 4.2.2.4);
- Elaboración de planes de implementación separados para cada punto de acción;
- Asignación de recursos humanos y financieros adecuados.

La autoridad del proyecto junto a los asesores debe desarrollar medidas y planes de implementación que apoyen a los objetivos estratégicos, así como identificar unidades o funcionarios concretos como propietarios ("propietarios de la acción"). Los propietarios de la acción deben ser representantes de los organismos o unidades más relevantes para la acción que se les ha asignado y tengan las mejores capacidades para implementarlas con éxito.
Estos funcionarios o unidades serían responsables y rendirían cuenta de la implementación del plan específico que se les asigne. Dado que se espera que los planes de implementación se ejecuten en el ámbito de trabajo, deben definirse de forma que los organismos que los implementen (propietarios de la acción) puedan comprenderlos claramente.
Puede ocurrir que la autoridad del proyecto tenga que coordinar la implementación de los distintos planes.

El comité rector puede tener que ayudar en la obtención de recursos adecuados para la implementación de los distintos planes. Esto garantizará que todos los esfuerzos realizados hasta el momento no sean en vano.

Se recomienda que los planes de implementación incluyan parámetros e indicadores de éxito específicos para controlar el progreso de las medidas.

4.5 Seguimiento y evaluación de la estrategia

En consonancia con los objetivos SMART (sección 4.1.5.4) de la estrategia contra la ciberdelincuencia, la autoridad del proyecto y los asesores también deben planificar el seguimiento y la evaluación de la estrategia a intervalos regulares, a fin de mantener el impulso de los avances. No realizar este seguimiento continuo de los trabajos de implementación puede poner en peligro tanto las medidas individuales como el proyecto en su totalidad.

El compromiso continuo de los propietarios de la acción y la notificación por parte de estos sobre los parámetros previamente definidos ayudarán a mantener el rumbo establecido para la implementación de la estrategia contra la ciberdelincuencia. El seguimiento debe centrarse en el progreso de las actividades de implementación, la disponibilidad de recursos y los problemas y riesgos

que puedan estar dificultando la implementación del plan. Cualquier retraso debe ser comunicado a la autoridad del proyecto con suficiente antelación para que puedan establecerse planes de atenuación. Por otro lado, la autoridad del proyecto también debe ser informada de los logros para que puedan ser reconocidos.

4.6 Ajustes de la estrategia e innovación

Al igual que el proceso inicial de redacción de la estrategia contra la ciberdelincuencia era un proceso iterativo, la estrategia finalizada también debe revisarse periódicamente para adaptarse a la nueva tecnología, los nuevos vectores de ataques y las necesidades en continua evolución del país.

Ejemplo: Evolución de la Estrategia de Ciberseguridad y contra la Ciberdelincuencia de Nueva Zelanda

El ejemplo del progreso de la estrategia contra la ciberdelincuencia de Nueza Zelanda ilustra el proceso que han emprendido muchos países con el fin de adoptar un marco de referencia que mantenga su pertinencia considerando las cambiantes tendencias económicas y sociales. Ilustra asimismo que la estrategia de lucha contra la ciberdelincuencia de un país debe estar en consonancia y adaptarse a un panorama más amplio de políticas nacionales, todas ellas sujetas a continuos ciclos de revisión.

La estrategia de 2011 de Nueva Zelanda sobre ciberseguridad mostraba la respuesta del gobierno ante el incremento de las ciberamenazas, definiendo áreas prioritarias e iniciativas y asignando los recursos apropiados.

En 2015 se publicó una Estrategia sobre Ciberseguridad renovada (segunda) acompañada de un Plan de Acción, remplazando a la Estrategia sobre Ciberseguridad de 2011. Asimismo, se emitió un **Plan Nacional para abordar la Ciberdelincuencia**[37] (similar a una Estrategia contra la Ciberdelincuencia) para garantizar una respuesta adecuada ante la ciberdelincuencia y definiendo las siguientes áreas prioritarias:

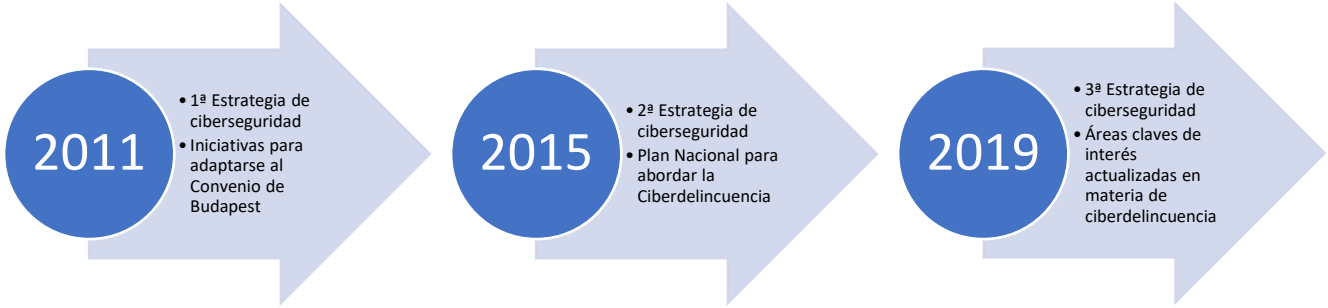
- desarrollar capacidades para abordar la ciberdelincuencia;
- adaptar las estructuras políticas y legislativas del país a la era digital;
- mejorar la respuesta operativa ante la ciberdelincuencia;
- utilizar las conexiones internacionales de Nueva Zelanda para combatir la ciberdelincuencia.

En 2019 Nueva Zelanda publicó su tercera Estrategia de Ciberseguridad[38] donde se actualizan las áreas prioritarias en materia de ciberseguridad, así como las áreas claves de interés en materia de ciberdelincuencia.

Figura 5: Plan Nacional de Nueva Zelanda para abordar la Ciberdelincuencia

37 https://dpmc.govt.nz/sites/default/files/2017-03/nz-cyber-security-cybercrime-plan-december-2015.pdf
38 https://dpmc.govt.nz/sites/default/files/2019-07/Cyber%20Security%20Strategy.pdf

Figura 6: Evolución de la estrategia de Nueva Zelanda en materia de ciberseguridad y ciberdelincuencia



5. Convenio de Budapest

Si bien el objetivo de una estrategia de lucha contra la ciberdelincuencia de un país es reforzar su capacidad global para combatir la ciberdelincuencia a nivel nacional, debe prestarse una atención particular a su armonización con normas y prácticas internacionales. Un país que esté en proceso de desarrollar o actualizar su estrategia debe intentar que su marco jurídico y otros objetivos estratégicos se correspondan con los requisitos de adhesión al acuerdo internacional más integral y coherente en materia de ciberdelincuencia y pruebas electrónicas, el Convenio sobre la Ciberdelincuencia del Consejo de Europa, conocido normalmente como Convenio de Budapest.

5.1 Acerca del convenio

El Convenio de Budapest es el primer tratado internacional sobre delitos cometidos a través de internet y otras redes informáticas. Trata particularmente delitos contra y mediante sistemas informáticos y datos, como el acceso ilícito, la interceptación ilícita, interferencia de datos y sistemas, fraude informático, material relacionado con la explotación sexual de niños u otras formas de violaciones de seguridad de las redes. Contiene, asimismo, una serie de poderes y procedimientos para las investigaciones judiciales y la obtención de pruebas electrónicas en relación a cualquier delito para el que las pruebas estén en un sistema informático, como conservación rápida de datos, búsquedas en redes informáticas o interceptación.

Su principal objetivo es lograr una política penal común cuyo fin es la protección de la sociedad frente a la ciberdelincuencia, especialmente mediante la adopción de legislación apropiada y el fomento de la cooperación internacional.[39] El convenio pretende principalmente:

(1) armonizar los elementos constitutivos de delito del derecho penal sustantivo nacional y disposiciones relacionadas en el ámbito de la ciberdelincuencia;

(2) aportar competencias de derecho procesal penal nacional necesarias para la investigación y el enjuiciamiento de dichos delitos, así como otros delitos cometidos mediante el uso de un sistema informático o pruebas relacionadas en formato electrónico; y

(3) establecer un régimen rápido y eficaz de cooperación internacional.[40]

El convenio quedó abierto para su firma en Budapest (Hungría) en noviembre de 2001. En 2003, se complementó con un protocolo sobre xenofobia y racismo cometidos a través de un sistema informático. Se espera que pronto esté disponible un segundo protocolo que permita mejorar la cooperación y la divulgación de pruebas electrónicas, incluyendo la cooperación directa con los proveedores de servicios y la cooperación en situaciones de emergencia.

39 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
40 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680occe5b

5.2 Ventajas del convenio

Todos los países pueden utilizar el Convenio de Budapest como directriz, lista de verificación o ley modelo. Sin embargo, pasar a ser Parte de este tratado conlleva ventajas adicionales:

- El Convenio ofrece un marco jurídico para la cooperación internacional en materia de ciberdelincuencia y pruebas electrónicas. El Capítulo III del tratado aporta disposiciones generales y específicas para la cooperación entre las Partes «en la mayor medida posible» no solamente en cuanto a la ciberdelincuencia (delitos contra y mediante ordenadores), si no con respecto a cualquier delito con pruebas electrónicas.
- Las Partes son miembros del Comité del Convenio sobre la Ciberdelincuencia (T-CY), e intercambian información y experiencias, evalúan la implementación del convenio o interpretan el convenio mediante notas de orientación.
- El T-CY también puede preparar protocolos adicionales a este tratado. Así, incluso si un Estado no participó en la negociación del tratado original, un Parte incorporada posteriormente puede participar en la negociación de futuros instrumentos, así como en la evolución del Convenio de Budapest.
- Las Partes del convenio se comprometen a establecer una cooperación fiable y eficaz. Los indicios muestran que entidades del sector privado cooperan más frecuentemente con las autoridades penales de las Partes del convenio, dado que las Partes deben contar con un marco jurídico nacional sobre ciberdelincuencia y pruebas electrónicas, incluyendo las garantías del Artículo 15.
- Los Estados que solicitan la adhesión o que se han adherido pueden convertirse en países prioritarios para los programas de capacitación. Esta asistencia de carácter técnico está pensada para facilitar la completa implementación del convenio y mejorar la capacidad para cooperar a nivel internacional.

5.3 Adhesión al convenio

Conforme al Artículo 37 del convenio, cualquier Estado puede unirse al tratado y pasar a ser Parte del tratado por «adhesión», si el Estado está preparado para poner en marcha las disposiciones establecidas en el convenio. El proceso de adhesión se desarrolla como sigue:

1 Una vez que esté disponible una ley (proyecto) que indique que un Estado ya ha implementado o probablemente implementará las disposiciones del Convenio de Budapest en su legislación nacional, el Ministro de Asuntos Exteriores (u otro representante autorizado) envía una carta al Secretario General del Consejo de Europa manifestando el interés de su Estado por adherirse al Convenio de Budapest.

2. El Consejo de Europa consulta seguidamente a las otras Partes y, una vez se haya alcanzado un acuerdo entre las Partes actuales del convenio, se invita al Estado a adherirse.

3. Las autoridades de ese Estado completan sus procedimientos internos, de forma similar a la ratificación de cualquier tratado internacional, antes de depositar el instrumento de adhesión en el Consejo de Europa.[41]

[41] https://rm.coe.int/cyber-buda-benefits-june2020a-en/16809ebe38

6. Modelo de Estrategia contra la Ciberdelincuencia

En este capítulo se propone un modelo para guiar a los redactores en las fases iniciales de creación de su propia estrategia contra la ciberdelincuencia. Aborda los puntos discutidos en los capítulos anteriores y ofrece algunas orientaciones adicionales sobre estructura y contenido.

Este modelo incluye elementos recomendados presentes normalmente en las estrategias contra la ciberdelincuencia, aunque aconsejamos a los redactores que tomen en consideración el contexto local y el marco regulador.

Existen cuatro componentes principales en una estrategia contra la ciberdelincuencia:

- Introducción
- Panorama actual de la ciberdelincuencia - evaluación y análisis
- Visión
- Áreas de interés, objetivos estratégicos y medidas.

6.1 Introducción

Esta primera sección es una introducción a la estrategia de lucha contra la ciberdelincuencia de un país. Debe permitir a los lectores comprender la naturaleza de la ciberdelincuencia en el país. Puede incluir subsecciones como las descritas más adelante.

6.1.1 Prólogo

Puede ser un mensaje de alguien que respalda e impulsa la estrategia, como el ministro competente u otro funcionario político de alto nivel. Esta introducción debería transmitir por qué la estrategia es importante y demostrar que cuenta con el apoyo y la aceptación de altos dirigentes, y que hay expectativa por ver los resultados. Asimismo, se debe presentar a la autoridad del proyecto.

6.1.2 Propósito del documento

Describe para qué se utilizará la estrategia y cómo ayudará al país.

6.1.3 Contexto para explicar por qué es necesaria la estrategia

Puede incluir una breve perspectiva de cómo han evolucionado en el país las estrategias sobre ciberdelincuencia, y aportar la justificación para la elaboración de la estrategia contra la ciberdelincuencia (ver sección 4.1).

Pueden citarse datos estadísticos (si los hubiera), como cifras sobre la incidencia de la ciberdelincuencia, el número de usuarios locales de internet y/o dispositivos móviles y el impacto financiero en el país y en víctimas concretas Estas cifras pondrán la situación actual de la ciberdelincuencia en perspectiva. Por otro lado, los datos estadísticos sobre la asimilación de las nuevas tecnologías pueden aportar una valiosa perspectiva de posibles futuros vectores de ataques de la ciberdelincuencia, por ejemplo, dispositivos IoT vulnerables.

En caso de que el país no cuente con una completa información sobre la ciberdelincuencia, se pueden utilizar cifras mundiales como un indicador.

6.2 Panorama actual de la ciberdelincuencia

6.2.1 Definiciones relacionadas con la ciberdelincuencia

Esta sección ofrece una clara definición de lo que el gobierno considera delitos dependientes de medios electrónicos, delitos facilitados por medios electrónicos y ciberseguridad (secciones 2.2 y 2.3). También puede hacer referencia a los distintos tipos de ciberdelincuentes o responsables de las amenazas (sección 3.4), y citar datos estadísticos sobre la ciberdelincuencia que puedan ser relevantes.

6.2.2 Datos estadísticos del país sobre ciberdelincuencia

Esta sección desglosa los datos estadísticos de alta calidad de la sección 5.1.3 según parámetros relevantes como tipo de delito, región, demografía, etc. Esto permitirá poner de relieve los delitos cibernéticos específicos y más frecuentes en el país.

Algunos ejemplos de cifras y tendencias que podrían incluirse aquí son:

- el número de ataques de delitos dependientes de medios electrónicos por tipo, por ejemplo, ataques de *ransomware* en un periodo de tiempo determinado;
- el número de delitos facilitados por medios electrónicos denunciados en un periodo de tiempo determinado;
- los principales tipos de ciberdelincuencia (desfiguración de un sitio web, *ransomware*, *phishing*, contenido sobre abuso de menores, acoso en línea, etc.);
- incremento de diferentes tipos de ciberdelincuencia en porcentaje y cifras reales en un periodo de tiempo determinado, por ejemplo, año a año.

El documento *Criminal Justice Statistics on Cybercrime and Electronic"Evidence*[42] establece el programa para la compilación de datos estadísticos de justicia penal con pasos claves para la recopilación de datos, el análisis y la cooperación entre múltiples partes interesadas.

6.2.3 Autoridades existentes en materia de ciberdelincuencia

Esta sección identifica a todos los organismos y autoridades pertinentes a nivel nacional y estatal/ provincial responsables de investigar, combatir y enjuiciar la ciberdelincuencia. Profundiza en sus cometidos dentro del sistema de justicia penal y sus mandatos (sección 4.2.2.1).

El objetivo es proporcionar una clara comprensión de la responsabilidad de cada autoridad, su jurisdicción, áreas de investigación, iniciativas y el ámbito de delitos cibernéticos que abarcan.

6.2.4 Legislación existente

Esta sección de la estrategia contra la ciberdelincuencia presenta la legislación sobre ciberdelincuencia que ya se ha promulgado (sección 4.2.2.2).

Puede incluir:

- leyes o normas sobre ciberseguridad;
- leyes sobre delitos informáticos;
- derecho penal sustantivo;
- derecho procesal (provisión de datos básicos de los abonados, datos sobre el tráfico, información sobre contenido);

[42] https://www.interpol.int/content/download/15731/file/Guide%20for%20Criminal%20Justice%20Statistics%20on%20Cybercrime%20and%20Electronic%20Evidence.pdf

- leyes y/o acuerdos de cooperación internacional como los Tratados de Asistencia Judicial Recíproca (MLAT);
- leyes sobre protección de datos, inclusive las normas sobre conservación de datos para responsables de la conservación de datos y del tratamiento de datos;
- cualquier otra ley que otorgue autoridad para la prevención, investigación o enjuiciamiento de la ciberdelincuencia.

6.2.5 Resumen de la autoevaluación y el análisis

Esta sección incluye los resultados del proceso de autoevaluación y análisis descrito en la sección 4.2.2.3 que determina la capacidad de un país para combatir la ciberdelincuencia, así como cualquier laguna que deba subsanar. Esta evaluación servirá de fundamento para la identificación de las áreas de interés, objetivos estratégicos y medidas de la estrategia (sección 5.4).

6.3 Visión

En esta sección se establece una clara visión de gobierno para gestionar la ciberdelincuencia. Normalmente se presenta como un resumen del éxito estratégico deseado por el gobierno. Valgan de ejemplo:

- «La visión del Plan de Acción Nacional de Singapur en materia de Ciberdelincuencia es garantizar un entorno en línea seguro y protegido para Singapur. Lo lograremos disuadiendo, detectando y desorganizando eficazmente las actividades de la ciberdelincuencia» - Plan de Acción Nacional de Singapur en materia de Ciberdelincuencia (NCAP)[43];
- «Los ciudadanos, los negocios y el gobierno pueden disfrutar de todos los beneficios de un espacio cibernético seguro, protegido y resiliente: trabajando juntos, en casa o en el extranjero, para comprender y abordar los riesgos, para reducir los beneficios de delincuentes y terroristas, y para aprovechar las oportunidades del ciberespacio para mejorar la seguridad y la resiliencia global del Reino Unido». – Estrategia contra la Ciberdelincuencia del Ministerio del Interior del Reino Unido[44];
- «La visión de la estrategia contra la ciberdelincuencia de la Real Policía Montada del Canadá es reducir la amenaza, el impacto y la victimización de la ciberdelincuencia en Canadá mediante acciones de aplicación de la ley» - Estrategia contra la ciberdelincuencia de la Real Policía Montada del Canadá[45].

Esta visión debe establecer idealmente un claro enfoque que abarque a todos los órganos de gobierno y a toda la sociedad para combatir la ciberdelincuencia, especialmente por ser una responsabilidad compartida en la que el gobierno, los ciudadanos, los negocios y la sociedad civil trabajan juntos con el fin de disuadir, detectar y desorganizar la ciberdelincuencia. Cuanto más clara sea la visión, más fácil será para los dirigentes y las partes interesadas claves garantizar un enfoque completo, consistente y coherente.

6.4 Áreas de interés, objetivos estratégicos y medidas

Esta sección del documento formará la mayor parte de la estrategia contra la ciberdelincuencia. Parte de la autoevaluación y el análisis (sección 4.2.2.3) y, basándose en los resultados, identificará las áreas de interés que el gobierno considera cruciales para luchar eficazmente contra la ciberdelincuencia. Posteriormente, se traducirán en objetivos estratégicos y en medidas (sección 4.2.2.4), que se asignarán a los organismos pertinentes (propietarios de la acción) y se supervisarán (sección 4.5).

---

43 https://www.mha.gov.sg/docs/default-source/press-releases/ncap-document.pdf
44 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf
45 https://www.rcmp-grc.gc.ca/wam/media/1088/original/30534bfob95ec362a454c35f154da496.pdf

6.4.1 Áreas de interés

Tal como se ha descrito, las áreas de interés resultan de la autoevaluación y el análisis (sección 4.2.2.3). Seguidamente, se explicarán los pormenores de estas áreas de interés y se aportarán definiciones claras, justificando asimismo las razones para esta selección.

6.4.2 Objetivos estratégicos

Pueden asociarse varios objetivos estratégicos para cada área de interés. Describen más específicamente lo que debe lograrse en un determinado periodo de tiempo.

6.4.3 Medidas

Las medidas son más específicas y detalladas que los objetivos estratégicos; incluyen plazos individuales, indicadores de éxito y un propietario asignado para garantizar la rendición de cuentas. Más de un punto de acción pude contribuir a un objetivo estratégico.

6.4.4 Ejemplos de objetivos estratégicos y sus medidas correspondientes

La siguiente sección ofrece ejemplos para los países que quieran desarrollar los objetivos estratégicos de su estrategia contra la ciberdelincuencia. Ver también la sección 4.2.2.4, particularmente la tabla 3.

6.4.4.1 Objetivo estratégico 1: Desarrollar un marco jurídico más eficaz para investigar y enjuiciar la ciberdelincuencia

El marco jurídico de numerosos países no criminaliza eficazmente la ciberdelincuencia. En estas circunstancias, el número de casos de ciberdelincuencia continuará aumentando mientras que la legislación se queda atrás.

Un objetivo estratégico puede ser actualizar el marco jurídico e impulsar marcos o instrumentos internacionales para abordar los desafíos actuales a los que se enfrentan la investigación, la aplicación de la ley y la resolución judicial en materia de ciberdelincuencia.

Medidas con plazos y organismo ejecutor

- Redactar y presentar una ley sobre ciberdelincuencia dentro de un *periodo determinado* (organismos ejecutores potenciales: Ministerio de Derecho o Departamento de Interior o la Oficina del Fiscal General);
- Garantizar la adhesión al Convenio de Budapest sobre la Ciberdelincuencia en un plazo de dos años (organismos ejecutores potenciales: grupo especializado conjunto entre Ministerio de Derecho y Ministerio de Asuntos Exteriores).

6.4.4.2 Objetivo estratégico 2: Capacitar a las autoridades penales

Los delitos cibernéticos han aumentado en volumen y en complejidad, lo que crea una demanda adicional de formación continua para las autoridades penales (por ejemplo, policía, fiscales y jueces) que se ocupan de estos delitos. Al mismo tiempo, las pruebas digitales desempeñan un papel cada vez más importante en muchos tipos de delitos. Mantener la integridad de las pruebas digitales desde su recopilación hasta su presentación ante el tribunal es con frecuencia un componente clave para un enjuiciamiento efectivo.

Dado que los dispositivos digitales y las pruebas electrónicas son componentes de prácticamente todos los tipos de delitos, incluso los funcionarios no especializados de las fuerzas del orden necesitan conocimientos básicos sobre pruebas digitales, así como sobre la manera adecuada de obtenerlas.

Los fiscales y los jueces dependen de la legítima recogida de pruebas precisas y fiables para su presentación y admisión ante un tribunal. También las condenas a menudo dependen de que los fiscales y los jueces comprendan suficientemente bien las pruebas digitales.

Por tanto, un objetivo estratégico podría ser desarrollar capacidades relevantes entre las autoridades penales nacionales responsables de la prevención, investigación, enjuiciamiento y resolución judicial de la ciberdelincuencia.

Incrementar la capacidad de investigación de los funcionarios de las fuerzas del orden hará que sean más eficaces en la lucha contra la ciberdelincuencia, y puede simplificar la colaboración con otros organismos gubernamentales y el sector privado.

Aumentar la capacidad de fiscales y jueces les ayudará a interpretar correctamente las pruebas electrónicas, así como a presentarlas/admitirlas ante un tribunal.

Medidas con plazos y organismo ejecutor

- Establecer y revisar continuamente un programa de formación sobre ciberdelincuencia dirigido a las fuerzas del orden en un plazo de seis meses (organismo ejecutor sugerido: Ministerio del Interior/Ministerio de Seguridad Pública o similar);
- Realizar al menos cinco cursos al año sobre investigación de la ciberdelincuencia dirigidos a funcionarios de las fuerzas del orden, a empezar tras la implementación del programa de formación (organismo ejecutor sugerido: Ministerio del Interior/Ministerio de Seguridad Pública o similar);
- Establecer y realizar al menos un curso de formación sobre los aspectos fundamentales de las pruebas digitales para todos los jueces y fiscales que traten casos de ciberdelincuencia, a comenzar dentro de un plazo de ocho meses (organismo ejecutor sugerido: Ministerio de Derecho, Oficina del Fiscal General).

6.4.4.3 Objetivo estratégico 3: Fomentar las asociaciones para combatir la ciberdelincuencia

Aunque el personal que trabaja en materia de ciberdelincuencia y ciberseguridad tiene la responsabilidad de intentar lograr un ciberespacio más seguro, no pueden lograrlo por sí mismos. La ayuda de otros organismos nacionales, otros países y otros sectores puede ser crucial para mejorar sus conocimientos y capacidades.

Colaboración intragubernamental

Algunos organismos tienden a trabajar de forma compartimentada, y lo mismo puede ocurrir con el intercambio de información entre organismos nacionales. Los conocimientos, la inteligencia y los recursos con frecuencia están dispersos en distintos organismos, y hay poco conocimiento y poca coordinación entre ellos en cuanto a la información, las iniciativas, las investigaciones y las capacidades.

Un objetivo estratégico podría ser promover el intercambio interinstitucional de información y recursos, lo que podría llevar a un enfoque significativamente más eficaz de la lucha contra la ciberdelincuencia.

Colaboración intergubernamental

Los delincuentes se comunican y operan a través de las fronteras sin restricciones, lo que les da ventaja sobre las autoridades encargadas de llevarlos ante la justicia.

Un objetivo estratégico para un país podría ser ampliar el uso de las redes internacionales, como redes de funcionarios de las fuerzas del orden y fiscalías. Estas redes a menudo intercambian información

de forma recíproca mediante mecanismos de diverso nivel de formalidad, haciendo que sus trabajos sean más eficaces.

Las fuerzas del orden nacionales cuentan con distintos mecanismos de cooperación a su disposición, desde formales como los MLAT a más informales, a fin de acelerar la transferencia de información entre organismos. Asimismo, se han desarrollado redes 24/7, como el sistema I-24/7 de INTERPOL, la red 24/7 del G8 contra la delincuencia de alta tecnología y la red 24/7 de contactos de las partes del Convenio de Budapest sobre la Ciberdelincuencia. Su objetivo es recibir solicitudes urgentes de pruebas digitales y facilitar la cooperación internacional.

Existen también mecanismos específicos para fiscales que trabajan en materia de ciberdelincuencia, como la red *Global Prosecutors E-Crime Network* (GPEN) de la Asociación Internacional de Fiscales.

Asociaciones público-privadas

La prevención y la investigación de incidentes cibernéticos complejos requieren unas habilidades y unos recursos importantes que pueden estar más fácilmente disponibles en organizaciones del sector privado que en las fuerzas del orden.

Una colaboración más sólida y de múltiples niveles entre el sector público y el sector privado contribuirá a mejorar la respuesta del país ante la ciberdelincuencia, y un público mejor informado hará que disminuya el número de víctimas potenciales.

Un objetivo estratégico podría ser crear asociaciones público-privadas entre diferentes sectores para beneficio de la prevención de la ciberdelincuencia y de las investigaciones judiciales. Estas asociaciones con entidades como proveedores de telecomunicaciones, servicios financieros y empresas de ciberseguridad pueden centrarse en diferentes aspectos como sensibilización, formación técnica, análisis y ayuda a la investigación mediante el intercambio de información e inteligencia. Podría incluir temas como información sobre ciberamenazas, tendencias, vulnerabilidades y cómo abordar determinados incidentes.

Un objetivo estratégico adicional podría ser sensibilizar al público en general sobre ciberamenazas comunes. Las iniciativas público-privadas como el programa del Reino Unido *Get Safe Online*[46] ofrecen al público consejos prácticos sobre cómo protegerse a sí mismos, a sus ordenadores y dispositivos móviles y a sus negocios de fraudes, usurpaciones de identidad, virus y muchos otros problemas que pueden encontrar en internet.

Asociaciones con organizaciones multinacionales

Las asociaciones con las organizaciones adecuadas pueden tener un efecto directo en la capacidad de un país para combatir la ciberdelincuencia, pues ofrecen oportunidades para el intercambio de información e inteligencia que puede ayudar en las investigaciones y en otras áreas. También pueden tener un efecto indirecto mediante la toma de contactos y el intercambio de recursos en forma de donaciones de equipo o puestas a disposición temporales de personal en determinadas organizaciones socias. Los socios internacionales y regionales pueden ofrecer además vías para la capacitación y el intercambio de buenas prácticas. Un ejemplo de ello es esta Guía.

Un objetivo estratégico podría ser establecer y mantener asociaciones relevantes a nivel mundial y regional.

A nivel mundial, organizaciones como INTERPOL, ONUDD, UIT, el Banco Mundial y los Centros de puesta en común y análisis de la información (ISAC) pueden ser socios valiosos.

[46] ttps://www.getsafeonline.org

A nivel regional, asociaciones con organizaciones como ASEAN o ASEANAPOL, Europol, la Unión Africana, la Organización de los Estados Americanos (OEA), la Organización de Cooperación Económica, la Comunidad del Caribe (CARICOM) y la Agencia de Implementación para Crimen y Seguridad (IMPACS), por nombrar algunas, pude ser muy beneficioso.

Medidas con plazos y organismo ejecutor

- Crear un centro de intercambio de información sobre ciberdelincuencia, que sea un órgano central que armonice el trabajo de las distintas partes interesadas nacionales implicadas en la investigación y el enjuiciamiento de incidentes de ciberdelincuencia. Debería incluir también un único conducto de información sobre delitos a fin de prevenir la duplicación de investigaciones. Implementación en un plazo de 12 meses, dirigido por los ministerios pertinentes;
- Alentar y optimizar el uso de las redes 24/7 relevantes, con efecto inmediato. Los organismos ejecutores son los responsables de la operación del sistema de justicia penal, por ejemplo, Ministerio del Interior/Ministerio de Seguridad Pública, Ministerio de Justicia;
- Facilitar la celebración de acuerdos formales de intercambio de inteligencia en un plazo de seis meses entre entidades pertinentes del sector público y privado, para ayudar a identificar ciberamenazas contra sectores críticos como energía, agua, atención sanitaria, comunicación, finanzas, transporte, etc. Ejecutor potencial: Unidad Nacional contra la Ciberdelincuencia;
- Promover una correcta ciberhigiene mediante campañas de sensibilización como *Safer Internet Day*, celebrada anualmente[47] en febrero. Implementación en un plazo de seis meses; ejecutores potenciales: Agencia Nacional para la Ciberseguridad y Unidad Nacional contra la Ciberdelincuencia;
- Explorar exhaustivamente y aprovechar la información y la inteligencia disponible de, o a través de, organizaciones como INTERPOL; por ejemplo, el Grupo Mundial de INTERPOL de Especialistas en Ciberdelincuencia (IGCEG) y los Informes sobre Ciberdelincuencia (CAR) con efecto inmediato. Organismo ejecutor: Unidad Nacional contra la Ciberdelincuencia o ministerio pertinente.

6.4.5 Anexos

5.4.5.1 Glosario

Puede resultar útil que la estrategia contra la ciberdelincuencia incluya también un glosario que defina términos claves, abreviaturas y acrónimos.

5.4.5.2 Referencias

Enlaces a referencias que pueden aportar orientaciones adicionales.

47 https://www.saferinternetday.org/

Anexo A: Estrategias y normas nacionales sobre ciberdelincuencia y ciberseguridad

En este anexo se ofrece una lista de referencias y recursos que se encuentran a disposición pública y a los que los países pueden recurrir cuando preparen sus propias estrategias contra la ciberdelincuencia. Algunos países han decidido no difundir sus estrategias contra la ciberdelincuencia, lo cual es una opción si su divulgación pública produce inquietud.

En muchos casos, se elabora una estrategia contra la ciberdelincuencia como complemento de la estrategia de ciberseguridad. En otros casos, ya hay una estrategia contra la ciberdelincuencia como parte de la estrategia de ciberseguridad.

Australia

- Estrategia de Ciberseguridad (2020) https://cybersecuritystrategy.homeaffairs.gov.au/AssetLibrary/dist/assets/images/PMC-Cyber-Strategy.pdf

Canadá

- Estrategia Nacional de Ciberseguridad (2018) hhttps://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf
- Estrategia contra la ciberdelincuencia de la Real Policía Montada del Canadá (2014) http://www.rcmp-grc.gc.ca/wam/media/1088/original/30534bf0b95ec362a454c35f154da496.pdf

Europa/Unión Europea

- Convenio de Budapest y normas relacionadas (2001) https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561
- Agencia de la Unión Europea para la Ciberseguridad (ENISA) - *NCSS Good Practice Guide: Designing and Implementing National Cyber Security Strategies* (2016) https://www.enisa.europa.eu/publications/ncss-good-practice-guide/at_download/fullReport

Nueva Zelanda

- Plan Nacional para abordar la Ciberdelincuencia (2015) https://dpmc.govt.nz/sites/default/files/2017-03/nz-cyber-security-cybercrime-plan-december-2015.pdf
- Estrategia de Ciberseguridad (2019) https://dpmc.govt.nz/sites/default/files/2019-07/Cyber%20Security%20Strategy.pdf

Singapur

- Estrategia de ciberseguridad de Singapur (2016) https://www.csa.gov.sg/-/media/csa/documents/publications/singaporecybersecuritystrategy.pdf

Reino Unido

- Estrategia Nacional de Ciberseguridad 2016-2021 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

- Estrategia contra la Ciberdelincuencia (2010) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf

Estados Unidos de América (2018)

- Estrategia Cibernética Nacional de los Estados Unidos de América https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

Unión Internacional de Telecomunicaciones (ITU)

- Guía para elaborar una Estrategia Nacional de Ciberseguridad (2018) https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

INTERPOL

ACERCA DE INTERPOL

La función de INTERPOL es posibilitar el trabajo conjunto de las policías de sus 194 países miembros para combatir la delincuencia transnacional y hacer del mundo un lugar más seguro. INTERPOL mantiene bases de datos mundiales con información policial sobre delincuentes y delitos, y proporciona apoyo operativo y forense, servicios de análisis y formación. Estas capacidades policiales se prestan en todo el mundo y sustentan tres programas generales: lucha contra el terrorismo, ciberdelincuencia, y delincuencia organizada y nuevas tendencias delictivas.

NUESTRA META: UNA "MAYOR COMUNICACIÓN POLICIAL PARA UN MUNDO MÁS SEGURO"

Nuestra meta es lograr un mundo en el que todos los profesionales de los organismos encargados de la aplicación de la ley sean capaces, a través de INTERPOL, de transmitir, intercambiar y consultar de forma segura información policial vital cuando y donde lo necesiten, garantizando así la seguridad de los ciudadanos de todo el planeta. Proporcionamos y promovemos constantemente soluciones avanzadas e innovadoras para hacer frente a los desafíos que se plantean a escala mundial en el ámbito policial y de la seguridad.