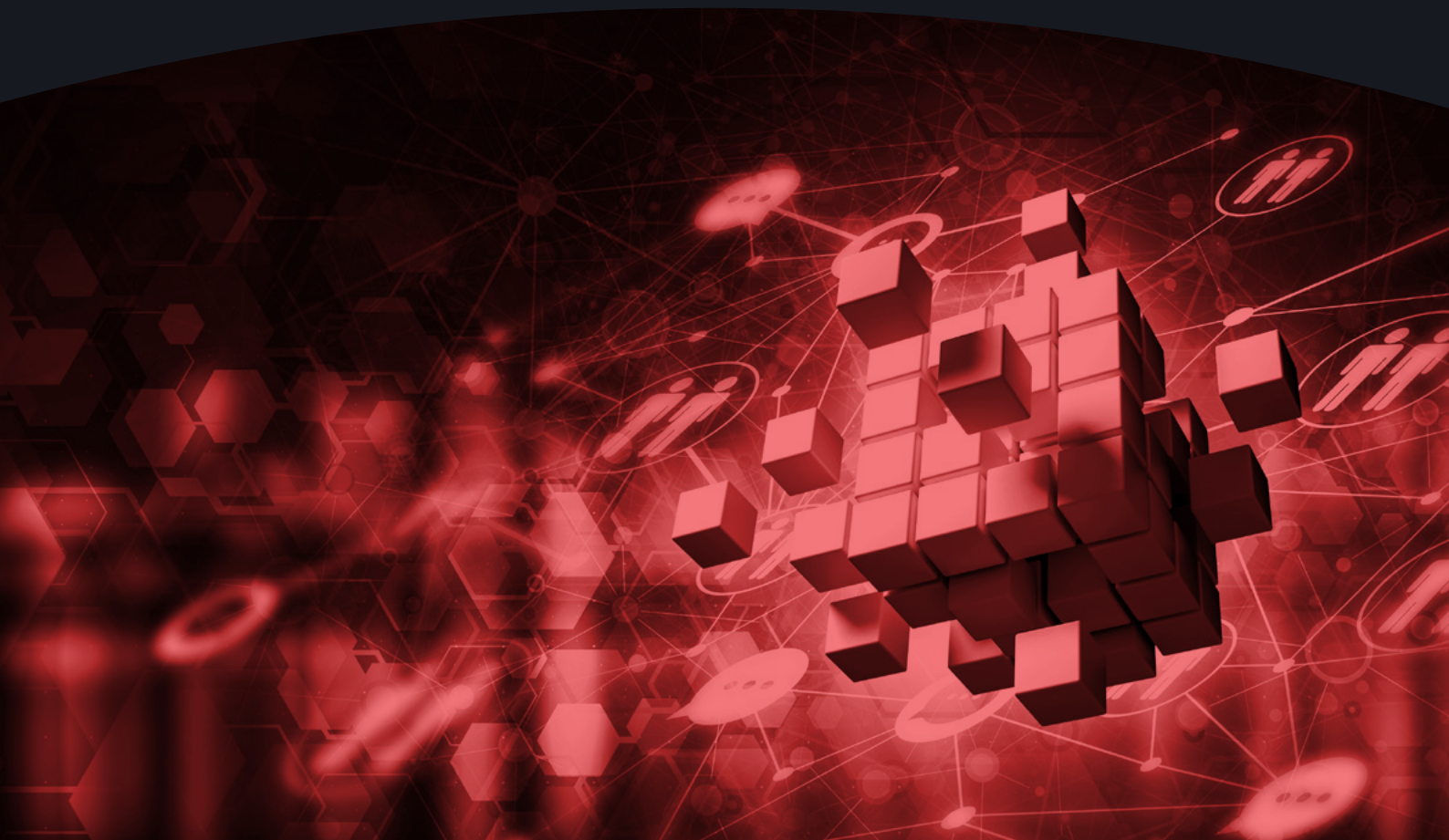
UNIDIR

¿Qué se necesita para crear capacidades cibernéticas?

Parte II. Introducción a un Enfoque Basado en Amenazas

SAMUELE DOMINIONI · GIACOMO PERSI PAOLI



Agradecimientos

El apoyo de los principales contribuyentes de UNIDIR sustenta todas las actividades del Instituto. Este estudio forma parte de la línea de trabajo de ciberestabilidad del Programa de Seguridad y Tecnología de UNIDIR, financiado por Microsoft y los gobiernos de Chequia, Francia, Alemania, Italia, los Países Bajos, Suiza y el Reino Unido, y por Microsoft.

UNIDIR desea expresar su agradecimiento al Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo (CICTE) de la Organización de los Estados Americanos (OEA) por traducir esta investigación y ponerla a disposición en español. Este informe se publicó originalmente en inglés en Julio 2023, que es la versión confiable; en el caso de divergencia, el texto en inglés prevalecerá.

Acerca de UNIDIR

El Instituto de las Naciones Unidas de Investigación sobre el Desarme (UNIDIR, por sus siglas en inglés) es un instituto autónomo de las Naciones Unidas financiado con contribuciones voluntarias. UNIDIR, uno de los pocos institutos de políticas en todo el mundo que se concentra en el desarme, genera conocimientos y promueve el diálogo y la acción en materia de desarme y seguridad. Con sede en Ginebra, UNIDIR ayuda a la comunidad internacional en el desarrollo de las ideas prácticas e innovadoras necesarias para encontrar soluciones a problemas críticos de seguridad.

Nota

Los Autores

Samuele Dominioni

Investigador, Programa de Seguridad y Tecnología

El Dr. Samuele Dominioni es investigador en el Programa de Seguridad y Tecnología de UNIDIR. Antes de unirse a UNIDIR ocupó cargos de investigación en entornos académicos y de grupos de expertos. Tiene un Doctorado en relaciones internacionales e historia política de Sciences Po, Francia, y la Escuela de Estudios Avanzados IMT, Italia.

Giacomo Persi Paoli

Director de Programa, Seguridad y Tecnología

El Dr. Giacomo Persi Paoli es el Director del Programa de Seguridad y Tecnología de UNIDIR. Sus conocimientos especializados abarcan la ciencia y la tecnología con énfasis en las implicaciones de las tecnologías emergentes para la seguridad y la defensa. Antes de unirse a UNIDIR, Giacomo fue Director Asociado en RAND Europa, donde dirigió la cartera de ciencia, tecnología e innovación en defensa y seguridad, así como del Centro de Estudios de Prospectiva de RAND. Tiene un Doctorado en Economía de la Universidad de Roma, Italia, y una Maestría en Ciencias Políticas de la Universidad de Pisa, Italia.

Tabla de Contenido

Abreviaciones y Acrónimos

CBM	Medidas de Fomento de la Confianza
CERT/CSIRT	Equipo de respuesta a emergencias informáticas/Equipo de respuesta a incidentes de seguridad informática
DDOS	Denegación de servicio distribuida
FCC	Capacidades cibernéticas fundamentales
GEG	Grupo de Expertos Gubernamentales
TIC	Tecnologías de la información y la comunicación
LI	Ley Internacional
GTCA	Grupo de trabajo de composición abierta
UNIDIR	Instituto de las Naciones Unidas para la Investigación sobre el Desarme
ONUDA	Oficina de Asuntos de Desarme de las Naciones Unidas

Resumen Ejecutivo

Mientras los Estados continúan discutiendo los cuatro pilares clave del Marco para el Comportamiento Responsable del Estado en el uso de las TIC (en adelante, el Marco)—normas de comportamiento responsable, derecho internacional, medidas de fomento de la confianza y desarrollo de capacidades—continúan sin explorar dos aspectos clave:

a. la medida en que la implementación del Marco puede utilizarse para aumentar la seguridad y la resiliencia nacional, regional e internacional frente a amenazas específicas; y
b. cómo utilizar amenazas específicas para informar las iniciativas de creación de capacidad.

El panorama de amenazas en el dominio de las TIC está en constante evolución y se vuelve más complejo y sofisticado a la vez que las medidas de ciberseguridad continúan mejorando. Si bien se debe tener en cuenta que más del noventa por ciento de los ataques cibernéticos podrían prevenirse por medio de la aplicación sistemática de "higiene" básica de seguridad, el Marco puede proporcionar una importante capa adicional de resiliencia. De hecho, establecer las capacidades necesarias para implementar el Marco equiparía a los Estados con herramientas importantes que pueden contribuir a la prevención o mitigación de ciberamenazas específicas, así como al fortalecimiento de su resiliencia cibernética general.

Este informe es el segundo de un estudio de dos partes realizado por UNIDIR y tiene como objetivo fortalecer los vínculos entre el Marco y las capacidades de los Estados para prevenir o mitigar de manera efectiva el impacto de actividades maliciosas relacionadas con TIC. El informe se centra en el concepto de Capacidades Cibernéticas Fundamentales (FCC, por sus siglas en inglés), introducido en la primera parte del estudio, que se define como la combinación de políticas y regulaciones, procesos y estructuras, alianzas y redes, personas y habilidades, y tecnología necesaria para implementar el Marco.

Este informe propone un enfoque que permitiría a los gobiernos evaluar mejor su preparación para aprovechar el Marco y así prevenir o responder a actividades y amenazas maliciosas específicas de las TIC. El 'enfoque basado en amenazas' propuesto abarca tres pasos.

- **Paso 1. Evaluación de amenazas y riesgos:** en este paso, un gobierno dado debe clasificar, evaluar y priorizar las amenazas de las TIC que están afectando su territorio.
- **Paso 2. Análisis del marco:** con base en los resultados del Paso 1, los gobiernos deben considerar cuáles elementos del Marco serían más relevantes y aplicables a la evaluación de amenazas específicas.
- **Paso 3. Identificación y evaluación de las FCC:** sobre la base del Paso 2, una vez que se hayan identificado los elementos más relevantes del Marco de acuerdo con la evaluación de amenazas nacionales, los gobiernos pueden usar la lista de las FCC para identificar las capacidades específicas requeridas para abordar amenazas específicas. Una vez que se completa esta identificación, puede convertirse en una línea de base útil para evaluar hasta qué punto un Estado determinado podría aprovechar el Marco para prevenir o responder ante amenazas específicas.

Este enfoque se ilustra con el uso de tres escenarios: dos que se centran en diferentes tipos de actos maliciosos (ransomware -secuestro de datos- y denegación de servicio distribuida) y uno que se centra en un vector específico (manipulación de la cadena de suministro).

Independientemente del perfil de amenaza, deben considerarse relevantes y aplicables ciertas normas y capacidades fundamentales asociadas sin importar el escenario o la amenaza bajo consideración, específicamente la Norma A sobre cooperación interestatal y la Norma E sobre derechos humanos. El análisis de los tres escenarios se basa en este punto e identifica elementos de capacidad cibernética fundamentales específicos adicionales que parecen ser recurrentes en múltiples amenazas y en múltiples normas.

Desde una perspectiva de política y regulación, los Estados deben priorizar el desarrollo (y la revisión periódica) de estrategias y políticas nacionales integrales de seguridad cibernética que, en combinación con leyes adecuadas, permitan a los Estados tomar todas las medidas necesarias a nivel nacional e internacional para garantizar la protección del dominio de las TIC, incluso a través de cooperación con múltiples partes interesadas. Además, los Estados deben priorizar el desarrollo de posiciones integrales y públicas sobre cómo se aplica el derecho internacional al dominio de las TIC.

Desde una perspectiva de proceso, los Estados deben priorizar el desarrollo de mecanismos para facilitar la cooperación en asuntos relacionados con la seguridad de las TIC con todas las partes interesadas nacionales relevantes, incluidas las agencias gubernamentales, el sector privado, la comunidad técnica y la sociedad civil, según corresponda. Esto garantizaría no solo flujos de información oportunos, eficientes y efectivos en tiempos de crisis, sino también el acceso a activos de conocimiento que pueden aprovecharse según corresponda para compensar posibles carencias o falta de experiencia disponible en el sector público. De manera similar, los Estados deben desarrollar mecanismos para facilitar la cooperación y la información a nivel bilateral, regional e internacional. El desarrollo de procesos y mecanismos específicos permitiría la creación de **alianzas y redes funcionales.**

En relación con las estructuras, los Estados deberían priorizar el desarrollo y la sostenibilidad de **capacidades de respuesta a incidentes informáticos** nacionales totalmente operativos que son elementos insustituibles de la primera línea de defensa contra actos maliciosos relacionados con las TIC. Se podrían explorar diversos acuerdos a nivel nacional y regional entre CSIRT/CERT públicos y privados para dar cuenta de las limitaciones en recursos, habilidades o tecnologías. Además, los Estados deberían priorizar la identificación de **dependencias responsables** dentro del gobierno nacional para actuar como **puntos focales para temas de TIC a nivel político y técnico**, incluso con la creación de un Punto de Contacto Nacional dedicado. La presencia de un **dependencia con la autoridad y los poderes para investigar y enjuiciar** actos maliciosos relacionados con las TIC parece ser un requisito transversal.

Si bien todos los sectores sufren una escasez de habilidades cibernéticas, la implementación exitosa del Marco se basará en la capacidad de los Estados para desarrollar internamente, o acceder a través de asociaciones externas, **conocimientos técnicos y jurídicos adecuados** para poder gestionar de manera efectiva los incidentes de TIC a nivel nacional y garantizar el cumplimiento del Marco, pero también para comprometerse constructivamente con sus homólogos a nivel internacional en cuestiones relacionadas con la seguridad de las TIC. Esto también se convertirá en una demanda cada vez mayor para los diplomáticos, quienes deberían fortalecer su comprensión de los problemas de las TIC y contar con el apoyo de especialistas y asesores según sea necesario.

Finalmente, la implementación exitosa del Marco dependerá también de la capacidad de un Estado para acceder a una cierta cantidad de **tecnologías y soluciones técnicas** ya sea desarrollándolas a nivel nacional o accediendo a ellas a través de asociaciones con otros (por ejemplo, acuerdos bilaterales o regionales con otros Estados, o asociaciones público-privadas). Estas soluciones tecnológicas incluyen, pero no se limitan, a **capacidades para prevenir, detectar e interrumpir diferentes tipos de ataques** (por ejemplo, plataformas de inteligencia de amenazas, sistemas de alerta temprana) y soluciones para aumentar la confidencialidad, integridad y disponibilidad de sistemas y datos (por ejemplo, centros de datos basados en la nube).

1. Introducción

Las ventajas y oportunidades socioeconómicas que ofrece el desarrollo rápido y generalizado de las tecnologías de la información y la comunicación (TIC) conllevan nuevos riesgos y amenazas para los Estados miembros y la comunidad internacional en general. Como se destaca en los informes finales del Grupo de Trabajo de Composición Abierta (GTCA) 2019-2021 sobre desarrollos en el campo de la información y las telecomunicaciones en el contexto de la seguridad internacional, y el Grupo de Expertos Gubernamentales (GEG) sobre la promoción del comportamiento responsable del Estado en el ciberespacio en el contexto de la seguridad internacional, los incidentes dañinos a las TIC están aumentando en frecuencia y sofisticación, y están en constante evolución y diversificación. El primer informe de progreso anual del GTCA 2021-2025 también enfatizó las crecientes amenazas que representan las TIC para la infraestructura y los servicios críticos, y el riesgo que representan las tecnologías nuevas y emergentes.

En la cuarta sesión sustantiva del GTCA 2021-2025, celebrada en marzo de 2023, más de 60 delegaciones tomaron la palabra para hablar sobre el tema de las amenazas existentes y potenciales, el mayor número de contribuciones sobre este tema específico en la agenda. La combinación de (1) tensiones geopolíticas intensificadas, (2) actividades maliciosas relacionadas con TIC denunciadas por actores estatales, (3) incidentes de TIC graves perpetrados por grupos criminales sofisticados que apuntan a los servicios públicos y a la infraestructura crítica operada por el sector privado, y (4) el aumento de la concienciación sobre el impacto de las tecnologías emergentes, como la inteligencia artificial (IA) y la

computación cuántica, han aumentado la profundidad y la amplitud de los debates que mantienen los Estados en relación con las amenazas.

Sin embargo, sigue siendo limitada la medida en que dichas discusiones están vinculadas al contexto, alcance y propósito más amplios del GTCA. Mientras los Estados continúan discutiendo los cuatro pilares clave del Marco para el Comportamiento Responsable del Estado en el uso de las TIC (en adelante, el Marco)—normas de comportamiento responsable, derecho internacional, medidas de fomento de la confianza y desarrollo de capacidades—dos aspectos clave continúan sin explorar:

a. la medida en que la implementación del Marco puede utilizarse para aumentar la seguridad y la resiliencia nacionales, regionales e internacionales frente a amenazas específicas; y
b. cómo se pueden usar amenazas específicas para informar las iniciativas de creación de capacidad.

Este informe es el segundo de un estudio de dos partes realizado por UNIDIR cuyo objetivo es fortalecer los vínculos entre el Marco y la capacidad de los Estados para prevenir o mitigar de manera efectiva el impacto de actividades maliciosas relacionadas con TIC seleccionadas mediante el diseño de una herramienta para identificar mejor los requisitos y priorizar intervenciones para creación de capacidades.

Este informe se centra en el concepto de capacidades cibernéticas fundamentales (FCC) tal como se presentó y describió en el primer informe de este estudio.[1]

1 Refiérase a Samuele Dominioni y Giacomo Persi Paoli. 2023. Descubrir las necesidades de desarrollo de capacidades cibernéticas: Parte I. Clasificación de capacidades cibernéticas fundamentales. UNIDIR.

2. Resumen de Conceptos Clave

2.1 El Marco de Actuación del Comportamiento del Estado Responsable en el Uso de las TIC

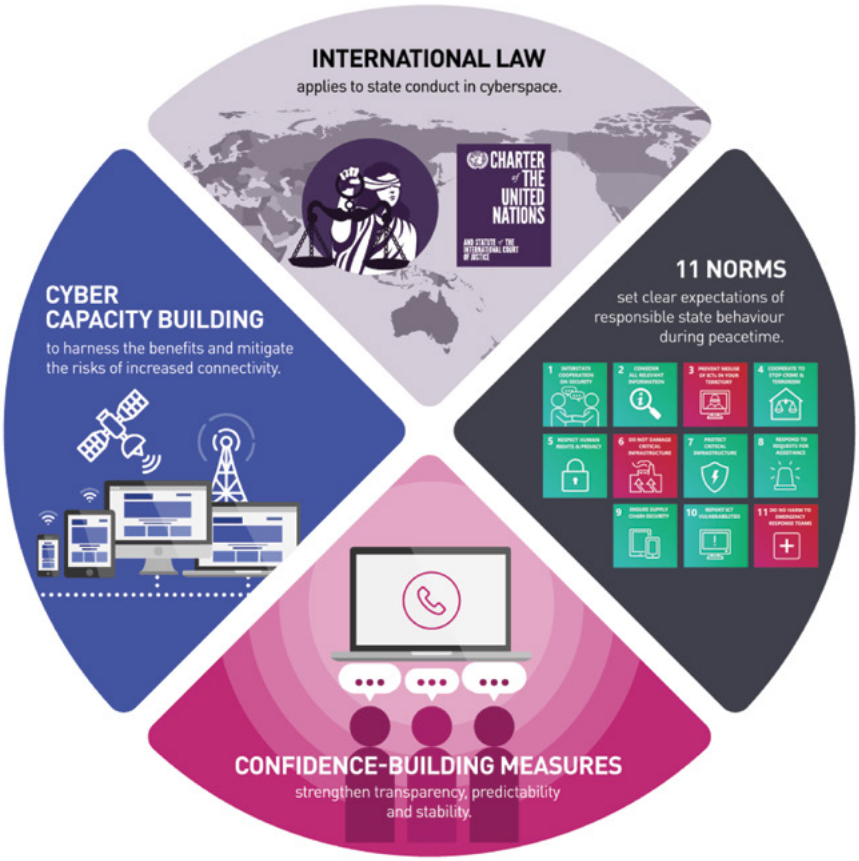
Durante las últimas dos décadas, los Estados miembros han estado discutiendo el uso de las TIC en el contexto de la paz y la seguridad internacionales. Tras el GEG de 2015, la Asamblea General desarrolló y adoptó un conjunto de 11 normas voluntarias no vinculantes de comportamiento responsable de los Estados[2] y los refinó aún más en procesos multilaterales posteriores.[3] Estas normas,

2 Ver A/RES/70/237.

3 Ver Informe sustantivo final del GTCA 2021, e Informe GEG 2021.

combinadas con la reafirmación de que el derecho internacional es aplicable al dominio de las TIC, con medidas dedicadas de fomento de la confianza (CBM por sus siglas en inglés) e iniciativas específicas de fomento de la capacidad y cooperación, forman los elementos del Marco para el Comportamiento del Estado Responsable en el ciberespacio (véase la figura 1).

Figura 1. El Marco de las Naciones Unidas para el Comportamiento Responsable de los Estados en el Ciberespacio



Fuente: https://www.internationalcybertech.gov.au/un-cyber-norms-resources

Un componente clave del Marco son las 11 normas voluntarias. Estas abordan una amplia gama de cuestiones relacionadas con la seguridad cibernética internacional e indican comportamientos que los Estados deben y no deben adoptar en el uso de las TIC para preservar la paz y la seguridad en el ámbito de las TIC. La Tabla 1 proporciona una descripción general de las 11 normas.

Tabla 1. Normas de Conducta del Comportamiento Responsable del Estado en el Ciberespacio[4]

	**Norma A** De conformidad con los propósitos de las Naciones Unidas, incluido el mantenimiento de la paz y la seguridad internacionales, los Estados deberían cooperar en la elaboración y aplicación de medidas para aumentar la estabilidad y la seguridad en el uso de las TIC y para prevenir prácticas de TIC que se reconozcan como dañinas o que puedan plantear amenazas a la paz y la seguridad internacionales.
	**Norma B** En caso de incidentes de TIC, los Estados deben considerar toda la información relevante, incluido el contexto más amplio del evento, los desafíos de la atribución en el entorno de las TIC y la naturaleza y el alcance de las consecuencias.
	**Norma C** Los Estados no deben permitir a sabiendas que su territorio se utilice para actos internacionalmente ilícitos utilizando las TIC.
	**Norma D** Los Estados deben considerar la mejor manera de cooperar para intercambiar información, ayudarse mutuamente, enjuiciar el uso terrorista y criminal de las TIC e implementar otras medidas de cooperación para hacer frente a tales amenazas. Es posible que los Estados deban considerar si es necesario desarrollar nuevas medidas a este respecto.
	**Norma E** Los Estados, al garantizar el uso seguro de las TIC, deben respetar las resoluciones del Consejo de Derechos Humanos 20/8 y 26/13 sobre la promoción, protección y disfrute de los derechos humanos en Internet, así como las resoluciones de la Asamblea General 68/167 y 69/166 sobre el derecho a la privacidad en la era digital, para garantizar el pleno respeto de los derechos humanos, incluido el derecho a la libertad de expresión.

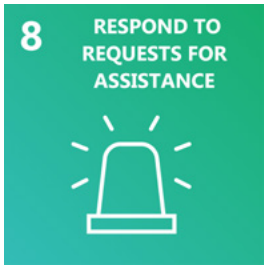
4 Iconos de: https://www.internationalcybertech.gov.au/un-cyber-norms-resources.

Norma F

Un Estado no debe realizar o apoyar a sabiendas una actividad de TIC contraria a sus obligaciones en virtud del derecho internacional que dañe intencionalmente la infraestructura crítica o perjudique de otro modo el uso y la operación de la infraestructura crítica para brindar servicios al público.

Norma G

Los Estados deberían tomar las medidas apropiadas para proteger su infraestructura crítica de las amenazas de las TIC, teniendo en cuenta la resolución 58/199 de la Asamblea General.



Norma H

Los Estados deben responder a las solicitudes apropiadas de asistencia de otro Estado cuya infraestructura crítica esté sujeta a actos de TIC malintencionados. Los Estados también deben responder a las solicitudes apropiadas para mitigar la actividad maliciosa relacionada con las TIC dirigida a la infraestructura crítica de otro Estado que emana de su territorio, teniendo en cuenta la soberanía.

Norma I

Los Estados deberían tomar medidas razonables para garantizar la integridad de la cadena de suministro de modo que los usuarios finales puedan confiar en la seguridad de los productos de TIC. Los Estados deben tratar de evitar la proliferación de herramientas y técnicas de TIC maliciosas y el uso de funciones ocultas dañinas.

Norma J

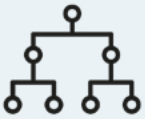
Los Estados deben alentar la notificación responsable de las vulnerabilidades de las TIC y compartir la información asociada sobre los recursos disponibles para dichas vulnerabilidades con el objetivo de limitar y posiblemente eliminar las amenazas potenciales a las TIC y la infraestructura dependiente de ellas.

Norma K

Los Estados no deben realizar ni apoyar a sabiendas actividades para dañar los sistemas de información de los equipos autorizados de respuesta a emergencias (a veces conocidos como equipos de respuesta a emergencias informáticas o equipos de respuesta a incidentes de seguridad cibernética) de otro Estado. Un Estado no debe utilizar equipos de respuesta de emergencia autorizados para participar en actividades internacionales maliciosas.

2.2 Capacidades Cibernéticas Fundamentales[5]

Las Capacidades Cibernéticas Fundamentales (FCC, por sus siglas en inglés), se definen como la combinación de políticas y regulaciones, procesos y estructuras, alianzas y redes, personas y habilidades, y tecnología necesaria para implementar el Marco. A los efectos de este estudio, estos cinco pilares se definen de la siguiente manera:

Políticas y Regulaciones 	Documentos oficiales relacionados con cuestiones de ciberseguridad. Estos incluyen documentos que describen las posiciones de los Estados miembros, políticas, estrategias (desarrolladas específicamente para sectores clave, por ejemplo, infraestructura crítica, o para aplicaciones intersectoriales a nivel nacional), marcos legales y regulatorios, y firmas de acuerdos u otras formas de cooperación con partes interesadas internacionales.
Procesos y Estructuras 	Cargos clave, organismos/entidades responsables, otros mecanismos nacionales o regionales y procesos, procedimientos y protocolos oficiales relacionados con la ciberseguridad.
Alianzas y Redes 	Iniciativas a nivel nacional e internacional dirigidas a fortalecer la capacidad nacional. A nivel nacional, incluye mecanismos o instrumentos de cooperación intrasectorial e intragubernamental. A nivel internacional, mecanismos o instrumentos de cooperación bilateral, regional y multilateral.
Personas y Habilidades 	Conocimientos y experiencia relacionados con la ciberseguridad. Cabe señalar que ciertas FCC enumeradas en el pilar de "personas y habilidades" también podrían cumplirse mediante la subcontratación y el establecimiento de acuerdos con proveedores externos u otras partes interesadas, en caso de que el Estado no pueda desarrollar o mantener esta capacidad especializada internamente.

5 Esta sección es un extracto de la primera parte de este estudio presentado en Samuele Dominioni y Giacomo Persi Paoli. 2023. Descubrir las necesidades de desarrollo de capacidades cibernéticas: Parte I. Clasificación de capacidades cibernéticas fundamentales. UNIDIR.

Tecnología 	Soluciones/capacidades técnicas a nivel nacional relacionadas con la ciberseguridad. Cabe señalar que las FCC enumeradas en el pilar de 'tecnología' también podrían cumplirse mediante la subcontratación a proveedores de servicios externos a través de, por ejemplo, asociaciones público-privadas.

La lista de FCC no pretende ser representativa de las mejores prácticas o medidas deseables. **Ha sido desarrollada con la idea de servir como línea base sobre la cual se podrían desarrollar respuestas más refinadas y completas** una vez que se alcance dicha línea base. Por lo tanto, las FCC representan **requisitos mínimos de capacidad necesarios para la implementación del Marco**, no las soluciones óptimas o las respuestas ideales. Como tal, los elementos que no surgieron como verdaderamente necesarios o fundacionales, sino más aspiracionales, deseables o 'avanzados', no se incluyeron en la lista. Además, también es importante señalar que se hace hincapié en cuál capacidad debe estar presente más que en cómo desarrollarla, que sigue siendo una prerrogativa nacional. Se puede consultar una descripción general de la lista completa de FCC para cada elemento del Marco en el Anexo A y se brindan explicaciones más detalladas de cada FCC en el primer informe de este estudio.[6]

6 Samuele Dominioni y Giacomo Persi Paoli. 2023. Descubrir las necesidades de desarrollo de capacidades cibernéticas: Parte I. Clasificación de capacidades cibernéticas fundamentales. UNIDIR.

3. Introducción al Enfoque Basado en Amenazas

Como se mencionó en el Capítulo 1, el panorama de amenazas en el dominio de las TIC está en constante evolución y se vuelve más complejo y sofisticado a medida que la base de referencia de las medidas de seguridad cibernética es cada vez más alta. Si bien cabe señalar que más del noventa por ciento de los ataques cibernéticos podrían prevenirse[7] mediante la aplicación sistemática de 'higiene' de seguridad básica (por ejemplo, cambiar las contraseñas predeterminadas, usar autenticación multifactor, usar antimalware, instalar actualizaciones de seguridad rápidamente, entre otros), el Marco para el comportamiento responsable del Estado puede proporcionar una capa adicional importante de resiliencia. De hecho, establecer las capacidades necesarias para implementar el Marco equiparía a los Estados con herramientas importantes que pueden contribuir a la prevención o mitigación de ciberamenazas específicas, así como al fortalecimiento de su resiliencia cibernética general.

7 Existen diferentes estimaciones por parte de varias empresas de ciberseguridad y tecnología. Por ejemplo, el Informe de defensa digital de Microsoft publicado en noviembre de 2022 estima que la higiene de seguridad básica aún protege contra el 98% de los ataques; ver https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022.

En la última década, se han desarrollado y aplicado con éxito varias metodologías, modelos y enfoques para identificar cuáles elementos y pasos deben emprender los gobiernos para desarrollar o fortalecer sus capacidades nacionales de TIC.[8] Sin embargo, ningún modelo existente aborda específicamente la implementación del Marco considerando diferentes contextos nacionales y diferentes percepciones de amenazas.

En este contexto, este proyecto de investigación propone un enfoque que permitiría a los gobiernos evaluar mejor su preparación para aprovechar el Marco y así prevenir o responder a actividades y amenazas maliciosas específicas de las TIC. El 'enfoque basado en amenazas' propuesto abarca tres pasos:

- **Paso 1. Evaluación de amenazas y riesgos**: en este paso, un gobierno dado debe clasificar, evaluar y priorizar las amenazas de las TIC que están afectando su territorio. Para llevar a cabo este análisis, los gobiernos pueden basarse en fuentes nacionales (p. ej., informes de inteligencia sobre amenazas de su agencia/entidades de seguridad cibernética) y/u otras fuentes (p. ej., informes de inteligencia sobre amenazas proporcionados por empresas privadas). La amenaza debe tener en cuenta no solo el tipo de ataque o malware utilizado, sino también elementos más amplios, como los objetivos más vulnerables o expuestos, los diferentes tipos de actores de amenazas, la posible naturaleza transfronteriza de la propia amenaza o de las posibles respuestas, y otros. Es importante que dichas evaluaciones de amenazas consideren también escenarios de riesgo en los que el país no es necesariamente la víctima prevista del ataque, pero tal vez sirve como víctima instrumental, por ejemplo, como país de "tránsito" o ruta para un ataque destinado a otra persona. Un ejemplo de una herramienta que los gobiernos podrían usar para realizar una evaluación integral de amenazas y riesgos es la Taxonomía de Incidentes Maliciosos TIC de UNIDIR.[9]
- **Paso 2. Análisis del marco:** con base en los resultados del Paso 1, los gobiernos deben considerar cuáles elementos del Marco serían más relevantes y aplicables a la evaluación de amenazas específicas. Es importante reconocer que cada amenaza o incidente de TIC, incluso del mismo tipo, aunque tenga ciertos puntos en común, también se caracterizará por factores únicos. Sin embargo, al observar perfiles de amenazas más generales y no incidentes específicos y únicos, sería posible identificar cuáles normas, elementos del derecho internacional y medidas de fomento de la confianza serían más pertinentes.
- **Paso 3. Identificación y evaluación de las FCC:** sobre la base del Paso 2, una vez que se hayan identificado los elementos más relevantes del Marco con base en la evaluación de amenazas nacionales, los gobiernos pueden usar la lista de las FCC (refiérase al Anexo A) para identificar las capacidades requeridas para abordar amenazas específicas. Si todas las FCC enumeradas en cada elemento del Marco o solo una selección de ellas fueran aplicables dependería de

8 Refiérase al **Modelo de madurez de la capacidad de ciberseguridad de Oxford para las naciones** (CMM) y a la **Encuesta del Índice de Ciberseguridad Global de la Unión Internacional de Telecomunicaciones**.

9 Samuele Dominioni y Giacomo Persi Paoli. 2022. Una taxonomía de incidentes maliciosos TIC. UNIDIR. **https://unidir.org/publication/taxonomy-malicious-ict-incidents**.

la amenaza específica que se esté considerando. Una vez que se completa esta identificación, puede convertirse en una línea de base útil para evaluar hasta qué punto un Estado determinado podría aprovechar el Marco para prevenir o responder a ciberamenazas específicas.

Además de informar las prioridades de creación de capacidad al brindar otra perspectiva sobre las posibles brechas y necesidades, esta metodología también brinda dos beneficios adicionales. En primer lugar, los gobiernos podrían utilizarlo para realizar "verificaciones de salud" periódicas de sus arquitecturas de ciberseguridad para garantizar que sigan siendo adecuadas para su propósito a medida que evolucionan las amenazas. En segundo lugar, podría usarse para realizar ejercicios teóricos periódicos basados en escenarios (a nivel nacional o regional) que involucren a todas las partes interesadas relevantes para examinar la preparación y la resiliencia para prevenir o gestionar las amenazas nuevas y existentes.

Cabe señalar que este enfoque no pretende clasificar los componentes del Marco, ni siquiera las propias normas, por importancia. Todos los componentes del Marco son esenciales y deben tenerse en cuenta. Sin embargo, al observar escenarios de amenazas específicos, puede que diferentes capacidades sean más relevantes o aplicables que otras para hacer frente a circunstancias específicas. Algunas capacidades pueden incluso ser un requisito previo para otras.

Finalmente, es importante resaltar que los factores más allá de la lista de FCC, que se desarrolló exclusivamente con un enfoque en el Marco, afectarán en última instancia la capacidad de un Estado para prevenir o mitigar las ciberamenazas. Sin embargo, como se mencionó anteriormente en esta sección, desarrollar o fortalecer las capacidades para implementar el Marco contribuirá positivamente a la resiliencia cibernética general de un Estado.

4. El Enfoque Basado en Amenazas en Acción: Ejemplos Ilustrativos

Para desarrollar el enfoque basado en amenazas e ilustrar cómo se puede utilizar para identificar requisitos de capacidad específicos, el equipo del proyecto desarrolló tres escenarios de amenazas diferentes y los utilizó para realizar talleres dedicados con expertos internos y externos.[10]

Con base en el análisis de las discusiones más recientes sobre amenazas existentes y emergentes en el contexto del GTCA, se seleccionaron tres amenazas cibernéticas específicas como ejemplos

10 Los talleres de expertos externos e internos alternaron sesiones plenarias y grupos de trabajo para analizar, con el apoyo de escenarios dedicados, los tres estudios de caso con miras a clasificar elementos relevantes del Marco para FCC específicas y necesidades de desarrollo de capacidades relacionadas. Por ejemplo, utilizando ransomware como punto de entrada, los participantes en el taller analizaron el Marco para identificar normas relevantes, elementos de derecho internacional o medidas de fomento de la confianza que podrían aplicarse al escenario. Luego, seleccionaron los elementos de FCC más adecuados para hacer frente a la amenaza. Los datos de estos dos talleres fueron agregados y analizados. Durante un evento paralelo a la cuarta sesión del GTCA en Nueva York (6 al 10 de marzo de 2023), UNIDIR presentó los resultados preliminares del proyecto de investigación. Posteriormente, se realizaron verificaciones adicionales de los hallazgos con expertos externos.

ilustrativos para esta metodología: dos centradas en diferentes tipos de actos maliciosos (malware y denegación de servicio distribuida) y uno centrado en un vector específico[11] (manipulación de la cadena de suministro). En particular, los actos maliciosos relacionados con las TIC propuestos para este estudio son los siguientes.

a. **Operaciones de malware dirigidas a datos** (p. ej., ransomware, borradores de datos): software malintencionado que busca socavar la confidencialidad, la integridad o la disponibilidad de los datos. El ransomware es un tipo de malware que busca cifrar datos o amenaza con filtrar datos exfiltrados para obtener el pago de un rescate. Un limpiador es una clase de malware destinado a borrar ('limpiar', de ahí el nombre) el disco duro de la computadora que infecta, eliminando datos y programas de manera maliciosa.
b. **Acto de denegación de servicio distribuida (DDOS):** un tipo de operación cibernética en la que un actor malicioso tiene como objetivo hacer que una computadora, dispositivo o red no esté disponible interrumpiendo el funcionamiento normal del dispositivo al abrumarlo con solicitudes del sistema hasta que el tráfico normal no pueda procesarse, lo que resulta en una denegación de servicio.
c. **Manipulación de la cadena de suministro de software:** un acto que inyecta código malicioso en una aplicación o software para infectar a todos los usuarios. En la manipulación de la cadena de suministro de software, los actores maliciosos buscan aprovechar las relaciones de confianza entre clientes y proveedores, quienes pueden no saber que su software está infectado con un código malicioso cuando lo lanzan al público. El código malicioso se ejecuta con la misma confianza y permisos que el software original al que está conectado.

Además de la naturaleza específica del acto malicioso, los tres escenarios de amenazas incluyen variaciones de otros factores clave: **tipos de víctimas** (por ejemplo, operadores de infraestructura crítica, agencias gubernamentales, otros actores y usuarios del sector privado), incertidumbre sobre **participación de actores estatales como perpetrador** y **dimensiones transfronterizas** del incidente. No existe una lista estándar o recomendada de factores a considerar al pensar en amenazas. La taxonomía de UNIDIR de incidentes de TIC maliciosos ofrece una buena visión general de cuáles podrían ser estos factores, pero en última instancia es una elección que depende de los contextos nacionales o regionales.

Para agregar más realismo al ejercicio y estimular debates más específicos, los tres perfiles de amenazas se desarrollaron aún más en narrativas de escenarios cortos, basados en eventos reales, que se utilizaron para describir un incidente cibernético específico (aunque hipotético).

Cabe señalar que, independientemente de las amenazas, debe considerarse que algunos elementos del Marco y las capacidades asociadas aplican siempre por igual. Estas son la Norma A y la Norma E:

---

11 "Vector" se refiere al método de intrusión en un sistema o red; véase Samuele Dominioni y Giacomo Persi Paoli. 2022. Una taxonomía de incidentes maliciosos TIC. UNIDIR. **https://unidir.org/publication/taxonomy-malicious-ict-incidents**.

	**Norma A** Esta norma es siempre aplicable dado su carácter estratégico/de alto nivel que sustenta cualquier forma de cooperación entre los Estados en materia de seguridad internacional de las TIC y su implementación incluye elementos fundamentales, como los Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT) / Equipos de Respuesta a Emergencias Informáticas (CERT), que son fundamentales para garantizar la resiliencia cibernética nacional.
	**Norma E** Esta norma es siempre aplicable ya que el respeto por los derechos humanos sustenta el comportamiento de los Estados en el dominio de las TIC sin importar el escenario de amenaza.

Finalmente, vale la pena señalar que varias FCC se repiten en múltiples escenarios, a veces con matices más específicos, a veces como requisitos idénticos. Esto se debe al hecho de que se pretende que cada escenario se pueda leer como una sección independiente y, por lo tanto, se proporciona toda la información relevante.

4.1 Escenario 1: Ransomware

Perfil de Amenaza

Tipo	Ransomware
Víctima	Dos infraestructuras críticas del sector energético
Perpetrador	Grupo delictivo con posible participación de un actor estatal
Transfronterizo	Sí; las sedes de las infraestructuras están ubicadas en dos países diferentes, y la evidencia sugiere la participación de dos perpetradores diferentes, ambos con sede en terceros países

Descripción del Escenario

En este escenario, los perpetradores emplearon ransomware para llevar a cabo un acto malicioso relacionado con las TIC dirigido a dos infraestructuras críticas transnacionales en la industria del petróleo y el gas, con sede en dos países diferentes (País Alfa y País Beta). Este acto condujo a una reducción del sesenta por ciento en la distribución de petróleo y gas en el País Alfa. La nota de rescate exigía el pago de $10MM. El análisis preliminar realizado por las empresas de seguridad cibernética sugirió que el acto fue lanzado por un grupo de piratería criminal que opera en gran parte desde un tercer país (País Charlie). Posteriormente, un análisis forense adicional realizado por la unidad de aplicación de la ley de seguridad cibernética de País Alfa encontró que el malware mostraba un nivel de sofisticación y algunos marcadores específicos asociados con las capacidades, tácticas, técnicas y procedimientos cibernéticos de otro país, País Cero, aunque no se encontraron pruebas concluyentes. El País Alfa y el País Cero tienen un historial de relaciones diplomáticas difíciles debido a intereses geoestratégicos en conflicto.

Elementos del Marco Relevantes para el Escenario

Sobre la base de la investigación y la consulta con expertos, los siguientes componentes del Marco se han considerado particularmente relevantes para este escenario:

Norma B

Dada la complejidad del escenario, la incertidumbre sobre el perpetrador y la posible participación del País Cero, y el contexto geopolítico más amplio, la Norma B es particularmente relevante para ambos Estados víctimas (Alfa y Beta) que pueden desear atribuir el ataque a un actor específico.

Norma C

En el escenario, la evidencia inicial sugiere que el perpetrador, un grupo criminal de piratería, estaba operando desde el País Charlie. Como tal, la Norma C se vuelve muy relevante para el País Charlie, de quien se espera que actúe de conformidad con esta norma.

Norma D

Para poder tomar medidas en respuesta a la información disponible que apunta a la posible participación de un grupo delictivo basado en el País Charlie, es importante que los países objetivo (Alfa y Beta) y el País Charlie estén equipados con las capacidades necesarias para implementar la Norma D y así cooperar.

Norma F

Dado el objetivo de este ataque y el posible papel que jugaron el País Charlie y el País Cero, la norma F también es muy relevante.

Norma G

Reflejando la consideración hecha para la Norma F, la Norma G se vuelve muy relevante para los Países Alfa y Beta cuya infraestructura crítica ha sido atacada.

Medidas de Fomento de la Confianza

Dada la dimensión transnacional de los incidentes y la posible participación de otros dos países, es particularmente relevante la capacidad de implementar CBM que den soporte a la comunicación y la transparencia entre los Estados.

Ley Internacional

La mayoría de las normas consideradas relevantes para este escenario requieren para su implementación la formulación de interpretaciones nacionales claras de los conceptos legales (por ejemplo, la debida diligencia, la infraestructura crítica, el principio de no intervención).

FCC Relevantes Aplicables al Escenario

Políticas y Regulaciones	• En relación con **políticas y regulaciones** relevantes para este escenario, todos los países involucrados deberían haber elaborado una **interpretación nacional de todas las normas en cuestión** y su **comprensión de cómo se aplica el derecho internacional (DI) al dominio de las TIC**. • El País Alfa debe tener una política que describa la **metodología y definiciones para su atribución**. • Dadas las diferentes partes interesadas involucradas en el incidente, los **marcos que permiten el intercambio de información** con las partes interesadas comerciales y no gubernamentales relevantes son particularmente importantes (Normas D, G). • Teniendo en cuenta el papel de un grupo criminal en el escenario, los países involucrados en los incidentes deberían tener **estrategias, políticas y legislaciones apropiadas que establezcan disposiciones para prevenir, detectar e interrumpir el uso malicioso de las TIC** (Norma C) y que **permitan la cooperación** en la investigación y enjuiciamiento de actividades cibercriminales (Norma D). • Dada la naturaleza específica del ataque, tales políticas y estrategias también deben cubrir el tema de **seguridad de datos** para garantizar que se puedan implementar las medidas adecuadas para crear copias de seguridad y redundancias. • Los Países Alfa y Beta (países objetivo) deberían tener **sectores de infraestructura crítica designados y legislación aprobada sobre la protección de la infraestructura crítica** (Norma G). • Finalmente, los gobiernos del País Charlie y el País Cero deberían poder demostrar que sus **políticas y legislaciones nacionales están alineadas con la Norma F** y con el requisito de no dañar la infraestructura crítica. Como mínimo, **sería necesaria una interpretación pública propia de la norma.**
Procesos y Estructuras	• Los países Alfa y Beta, como países objetivo, deben desarrollar **estándares nacionales de prueba de atribución** (Norma B), así como procesos y procedimientos que permitan el **intercambio de información y cooperación entre entidades gubernamentales y no gubernamentales pertinentes** en todos los países involucrados, incluyendo protocolos especialmente para evidencia digital (Normas A, B, C, D, G). • En términos de estructuras, los países deben tener bien establecidos y en pleno funcionamiento **CSIRT/CERT nacionales o regionales** (Normas A, C, D, G, CBM) así como **Puntos de contacto a nivel diplomático y técnico** (Norma A, CBM) y un **mecanismo de supervisión independiente y eficaz** capaz de garantizar la transparencia y la rendición de cuentas para la operación del Estado (incluida la recopilación de datos) en el dominio de las TIC (Normas A, E, F y DI).

Alianzas y Redes	• Dentro de los países objetivo, la **cooperación intersectorial**, incluso con el sector privado, sería clave para resolver y recuperarse adecuadamente del acto malicioso de las TIC (Normas A). Esto debería incluir **cooperación transfronteriza con los propietarios y operadores de infraestructuras pertinentes** (Norma G). • Entre los países objetivo, sería esencial la **cooperación bilateral para garantizar el intercambio de información** (según las Normas A, B, C y F) e **investigaciones transfronterizas** (Norma D). • **La cooperación bilateral** también sería importante entre los países objetivo (Alfa y Beta) y los países potencialmente involucrados en el acto malicioso (Charlie y Vero) con un enfoque específico en **la solución de desacuerdos y disputas** (según Norma B) y sobre investigación (según Norma D).
Personas y Habilidades	• Para responder adecuadamente al escenario, los Países Alfa y Beta específicos requerirían expertos con habilidades para **gestionar incidentes de ciberseguridad** (Norma A) así como **realizar o evaluar investigaciones técnicas** de incidentes TIC (Norma B). El País Charlie también requeriría experiencia en la **identificación e interrupción de actos maliciosos en las TC** que emanen de su propio territorio (Norma C). • Además de las habilidades técnicas y de gestión de incidentes, es importante que todos los gobiernos involucrados tengan acceso a **experiencia legal** sobre la aplicabilidad del derecho internacional en el contexto de las TIC (Normas A, B, F e DI), así como **habilidades diplomáticas y de comunicación pública** específicas al contexto de las TIC y la infraestructura crítica (Normas B, C, G y CBM).
Tecnología	• Según el escenario, los países objetivo y el país desde el que opera el presunto grupo ciberdelincuente deben estar equipados con **capacidades técnicas para prevenir, detectar e interrumpir actos de TIC maliciosos**, particularmente contra la infraestructura crítica (Normas A, C, D, G). Los países objetivo del ransomware también requerirían soluciones tecnológicas para garantizar la redundancia y la copia de seguridad de los datos (por ejemplo, centros de datos basados en la nube).

4.2. Escenario 2: Denegación de Servicios Distribuida (DDoS)

Perfil de Amenaza

Tipo	Denegación de servicio distribuida (DDO)
Víctima	Sitios web y aplicaciones del gobierno
Perpetrador	Una Amenaza Persistente Avanzada (APT) con participación plausible de un actor estatal
Transfronterizo	Sí; los ataques se han enrutado a través de varios países

Descripción del Escenario

El País Alfa sufrió una campaña prolongada de múltiples ataques DDoS dirigidos a sus servicios públicos (incluidos los sistemas de seguridad social). Las primeras investigaciones de los incidentes destacaron que los actos maliciosos se canalizaron a través de computadoras y redes en otros dos países (Beta, Charlie). A medida que los ataques DDoS aumentaron en frecuencia y magnitud, el País Alfa declaró el estado de emergencia. Investigaciones adicionales realizadas por las autoridades del País Alfa vincularon los actos maliciosos relacionadas con las TIC con una APT conocida estrechamente asociada con el gobierno de un tercer país con intereses estratégicos en competencia (País Cero).

Elementos del Marco Relevantes para el Escenario

Sobre la base de la investigación y la consulta con expertos, los siguientes componentes del Marco se han considerado particularmente relevantes para este escenario:

Norma B

En este escenario, la combinación del enrutamiento de los ataques a través de terceros países, la potencial participación de una APT asociada a otro Estado y la gravedad del impacto que llevó a la declaración de emergencia nacional, puede llevar a la víctima (País Alfa) a considerar la opción de atribuir públicamente el ataque a otro Estado. En este caso, la Norma B es particularmente pertinente.

Norma C

Esta norma es particularmente relevante para los 'países de tránsito' en este escenario que juegan un papel clave en la interrupción del ataque.

Norma D

Para responder de manera efectiva a este escenario de amenaza, el país víctima y los países de tránsito deben poder implementar de manera efectiva la norma que llama a la cooperación para detener las actividades maliciosas perpetradas por la APT.

Medidas de Fomento de la Confianza

Dada la dimensión transnacional de los incidentes, la implementación efectiva de CBM, en particular de Puntos de Contacto bien establecidos y completamente operativos a nivel diplomático y técnico, sería particularmente relevante en la gestión de las respuestas tanto operativas como políticas al incidente.

Ley Internacional

El escenario de amenaza presentado en este caso, junto con las normas destacadas como relevantes, requiere que los países involucrados elaboren posiciones claras sobre temas clave de derecho internacional como la debida diligencia, el principio de no intervención y el principio de responsabilidad del Estado.

FCC Relevantes Aplicables al Escenario

Políticas y Regulaciones

- En cuanto a las políticas y regulaciones, como punto de partida, los países deberían tener **interpretaciones nacionales de los componentes del Marco aplicables a este escenario** (Normas B, C, D e DI). Esto proporcionará la base sobre la cual construir la respuesta específica.
- Además, existen varias políticas y regulaciones que los países deberían haber adoptado/implementado según su papel en el escenario. En lo que respecta a la Norma B sobre atribución, el País Alfa, como país víctima, debe tener una **clasificación de incidentes TIC en términos de escala e impacto** que podría sustentar la declaración del estado de emergencia y una **política de atribución**, incluidas las definiciones y la metodología.
- La norma C es particularmente relevante para los países de tránsito, que deberían tener **políticas y estrategias de ciberseguridad que describan disposiciones para prevenir, detectar e interrumpir actos de TIC maliciosos**, apoyado por **medidas legislativas adecuadas para investigar y enjuiciar** esos actos (Norma C y D).
- Todos los países involucrados también deberían haber establecido **reglamentos que permitan la cooperación y el intercambio de información** con entidades comerciales y no gubernamentales relevantes (Norma D).

Procesos y Estructuras	• Hay varios procesos y estructuras relevantes para este escenario. En términos de procesos, para apoyar la posible atribución del incidente a un tercer país (Norma B), el País Alfa debe desarrollar **normas nacionales de prueba**, y **procesos y procedimientos** (incluyendo protocolos en particular para el intercambio de evidencia digital) **con el objetivo de permitir el intercambio de información** entre las entidades gubernamentales y no gubernamentales pertinentes (Normas B, C y D). • En términos de estructuras, los países deberían tener **CSIRT/CERT nacionales o regionales** (Normas A, C, D). • Dada la dimensión transnacional de los ataques DDoS, también es crucial que los países Alfa, Beta y Charlie tengan **capacidades de aplicación de la ley cibernética** (Normas C, D), así como **mecanismos de cooperación** entre ellos (Norma A) para intervenir rápidamente e interrumpir las actividades maliciosas. • **Los Puntos Nacionales de Contacto** a nivel diplomático y técnico (Norma A, CBM) jugarían un papel clave en la gestión y resolución del incidente. • Finalmente, todos los Estados involucrados deben tener un **mecanismo de supervisión independiente y eficaz** capaz de garantizar la transparencia y la rendición de cuentas para la operación del Estado (incluida la recopilación de datos) en el dominio de las TIC (Normas A, E y DI).
Alianzas y Redes	• Para gestionar un ataque integral a las instituciones públicas, se requiere **cooperación intragubernamental y cooperación de múltiples partes interesadas** (Normas A, C). • **La cooperación internacional** enfocada en el **intercambio de información** (Normas A, B, C) e **investigación y enjuiciamiento** (Norma D) entre los países Alfa, Beta y Charlie sería imprescindible y requeriría la disponibilidad de **protocolos y mecanismos de cooperación.** • Al mismo tiempo, es crucial que se requiera la **cooperación y comunicación bilateral,** a través de **Puntos de contacto** y canales diplomáticos entre el País Alfa y el País Cero para gestionar las implicaciones políticas del incidente y trabajar hacia la solución de desacuerdos y disputas.

Personas y Habilidades	• Para responder adecuadamente al escenario, el país objetivo Alfa requeriría expertos con habilidades para **gestionar incidentes de ciberseguridad** (Norma A) y a **realizar o evaluar investigaciones técnicas** de incidentes de TIC en apoyo de la implementación de la Norma B. Los países Beta y Charlie también requerirían experiencia en la **identificación e interrupción de actos de TIC maliciosos** que emanen de su propio territorio (Norma C). • Además de las habilidades técnicas y de gestión de incidentes, es importante que todos los países involucrados tengan acceso a **experiencia legal** sobre la aplicabilidad del derecho internacional en el contexto de las TIC (Normas A, B, F y DI), así como **habilidades diplomáticas y de comunicación pública** específicas al contexto de las TIC para gestionar de manera efectiva las relaciones bilaterales con otros países involucrados y la comunicación pública más general con otros países y partes interesadas (Normas B, C, G y CBM).
Tecnología	• Los elementos tecnológicos relacionados con este escenario se refieren a **capacidades para prevenir, detectar e interrumpir los ataques DDoS** en el país víctima y en los países de tránsito. Estos podrían incluir, por ejemplo, soluciones de red de entrega de contenido para ayudar a absorber y desviar un ataque DDoS al distribuir el tráfico a través de múltiples servidores para mitigar el impacto de un ataque y prevenir un único punto de falla, o servicios de protección DDoS basados en la nube para detectar y mitigar los ataques en tiempo real, aprovechando la escalabilidad de la nube para manejar ataques a gran escala.

4.3. Escenario 3: Manipulación de la Cadena de Suministro

Perfil de Amenaza

Tipo	Malware (puerta trasera de la cadena de suministro)
Víctima	Un proveedor de software de ciberseguridad y miles de usuarios, incluidas instituciones públicas
Perpetrador	Actor estatal desconocido pero plausible
Transfronterizo	Sí; las víctimas están distribuidas por todo el mundo y la intrusión se enrutó a través de servidores en varios países

Descripción del Escenario

Una empresa de ciberseguridad con sede en País Alfa descubrió malware que había infectado una gran cantidad de sistemas de clientes. El malware parecía haber sido entregado a través de un acto de manipulación de la cadena de suministro dirigido a un proveedor de software externo (con sede en el mismo país) que sin darse cuenta distribuyó el malware de puerta trasera a través de una actualización de software programada. Más de 50.000 organizaciones públicas y privadas de todo el mundo utilizan el software en cuestión como herramienta de gestión empresarial. Como resultado, el ataque comprometió los datos, las redes y los sistemas de miles de organizaciones y usuarios y también expuso potencialmente a sus clientes y socios. Los análisis realizados por las autoridades de un grupo de países sugirieron que al administrar la intrusión a través de múltiples servidores ubicados en diferentes países e imitar el tráfico de red legítimo, los perpetradores pudieron eludir las técnicas de detección de amenazas empleadas por empresas privadas y por agencias gubernamentales, lo que denota un nivel de sofisticación propia de un actor estatal avanzado.

Elementos del Marco Relevantes para el Escenario

Sobre la base de la investigación y la consulta con expertos, los siguientes componentes del Marco se han considerado particularmente relevantes para este escenario:

Norma D

El malware apuntó a un proveedor de software en el País Alfa, pero el impacto fue mundial, lo que exigió la cooperación interestatal en la investigación y enjuiciamiento del incidente.

Norma G

Dada la gran escala y el impacto del acto malicioso, es esencial garantizar la protección de la infraestructura crítica contra los riesgos de la cadena de suministro.

Norma I

Dado que el escenario se basa en una cadena de suministro de software comprometida, esta norma es fundamental para el escenario.

Medidas de Fomento de la Confianza

Considerando la dimensión transnacional de los incidentes, en particular son pertinentes las medidas de fomento de la confianza especialmente diseñadas con el objetivo de apoyar una comunicación y un intercambio de información más eficientes entre los Estados.

Ley Internacional

A pesar de la falta de evidencia suficiente para atribuir el ataque a un perpetrador específico, el escenario de amenaza presentado en este caso, junto con las normas destacadas como relevantes, requieren que los Estados involucrados desarrollen posiciones claras sobre cuestiones clave de derecho internacional como la debida diligencia (particularmente en el País Alfa), el principio de no intervención y el principio de responsabilidad del Estado.

FCC Relevantes Aplicables al Escenario

Políticas y Regulaciones

- Todos los países involucrados en el incidente deberían haber adoptado e implementado **políticas y estrategias para prevenir, detectar e interrumpir actos maliciosos relacionados con las TIC,** apoyado por medidas legislativas adecuadas para investigar y enjuiciar esos actos (Norma D).
- Todos los países involucrados también deberían haber establecido **reglamentos que permitan la cooperación y el intercambio de información** con entidades comerciales y no gubernamentales relevantes (Norma D).
- Para salvaguardar la infraestructura crítica, los países deben tener una **designación nacional de infraestructura crítica**, política o estrategia de ciberseguridad con **disposiciones sobre reducción del riesgo cibernético, medidas de seguridad cibernética para productos de TIC que respalden operaciones de infraestructura crítica** y todas las demás medidas incluidas en la resolución 58/199 sobre cultura global de ciberseguridad y protección de infraestructuras críticas de información (Norma G).
- Además, en su política o estrategia de seguridad cibernética, los países deben abordar el **riesgo de la cadena de suministro** y proporcionar un **marco apropiado** para prevenirlo y mitigarlo (Norma I). Relacionado con este punto podría estar el desarrollo e implementación de **normas y estándares comunes para la seguridad de la cadena de suministro** (aunque esto va más allá del alcance de lo que puede lograr un solo país).

	• Otros elementos clave relevantes para este escenario de amenaza son el desarrollo de **regulaciones** que prohíban la introducción de funciones ocultas dañinas y la explotación de vulnerabilidades en productos de TIC y el desarrollo de **fuertes requisitos de seguridad de la cadena de suministro para que los proveedores** se incorporen en la gestión del ciclo de vida de los productos de seguridad y TIC (Norma I).
Procesos y Estructuras	• Particularmente importante para este escenario sería que todos los países involucrados desarrollen e implementen **mecanismos de gobernanza del riesgo de la cadena de suministro** que involucren a las partes interesadas clave que representan cada nodo de la cadena de valor para coordinar acciones y respuestas al acto malicioso (Norma I). • Además, para apoyar la comunicación efectiva entre las partes interesadas gubernamentales y no gubernamentales, los países deben desarrollar e implementar **procesos y procedimientos (incluidos protocolos especialmente para el intercambio de evidencia digital) para permitir el intercambio de información** (Norma D). Esto debe incluir procesos para adquirir, procesar y almacenar datos e información para la investigación y enjuiciamiento cibernéticos. • En términos de estructuras, es importante establecer Puntos de Contacto a nivel diplomático y técnico (Norma A) para permitir que los gobiernos de los países involucrados mantengan canales de comunicación abiertos y eficientes. • Los países también deberían tener **CSIRT/CERT nacionales (o regionales)** activos (Normas A, D, G) para mitigar el impacto y minimizar el tiempo de recuperación después del incidente y dichos CSIRT/CERT deben estar bien coordinados. • Además de la coordinación técnica entre CSIRT/CERT, es importante que los países hayan designado **organismos nacionales con facultades legales para investigar, enjuiciar y hacer cumplir el estado de derecho en relación con actos dolosos en el ámbito de las TIC**. Estas agencias deben poder interactuar y cooperar entre sí de manera efectiva según sea necesario (Normas A, D). • Por último, también es esencial un **mecanismo de supervisión** independiente y eficaz que asegure la transparencia y la rendición de cuentas para la operación del Estado (incluida la recopilación de datos) en el dominio de las TIC (Normas A, E).

Alianzas y Redes	• En lo que respecta a las asociaciones y redes, existen elementos importantes que los países deben establecer para abordar las amenazas de manipulación de la cadena de suministro. **La cooperación intersectorial entre organismos nacionales y el sector privado** (en el escenario: la empresa de ciberseguridad, el proveedor de software y otras partes interesadas relevantes) es clave para responder adecuadamente a los ataques a la cadena de suministro dirigidos, por ejemplo, a los procesos de actualización automática de seguridad (Normas A). • Además, son esenciales la **cooperación bilateral, regional y multilateral entre Estados** con el objetivo de intercambiar información para la investigación (incluso a través de redes técnicas y de aplicación de la ley) y el enjuiciamiento (Normas A, D), y para el intercambio de conocimientos sobre medidas para garantizar la integridad de la cadena de suministro (Norma I).
Personas y Habilidades	• Para responder adecuadamente al escenario, todos los países seleccionados requerirían expertos con habilidades para **gestionar incidentes de ciberseguridad** (Norma A) en particular los resultantes de una cadena de suministro comprometida (Norma I) y con miras a maximizar la eficiencia de la fase de respuesta y recuperación. • Además de las habilidades técnicas y de gestión de incidentes, es importante que todos los países involucrados tengan acceso a **experiencia legal** sobre la aplicabilidad del derecho internacional en el contexto de las TIC (Norma A) para garantizar posibles implicaciones legales del incidente, así como **habilidades diplomáticas y de comunicación pública** específicas al contexto de las TIC, en particular del país adonde se originó el ataque, para gestionar de manera efectiva las relaciones bilaterales con otros países involucrados y la comunicación pública más general con otros países y partes interesadas (Norma I).
Tecnología	• Los países y organizaciones objetivo deben estar equipados, o tener acceso a través de un socio externo, con la **capacidad técnica para prevenir, detectar o interrumpir ataques a la cadena de suministro**. Estas capacidades pueden incluir, entre otras, plataformas de inteligencia de amenazas, sistemas de alerta temprana e, idealmente, herramientas para la evaluación de productos TIC.

5. Conclusión

Los tres ejemplos presentados en el capítulo 4 proporcionan una ilustración de cómo las medidas específicas diseñadas para implementar el Marco para el Comportamiento del Estado Responsable en el ciberespacio podrían contribuir a prevenir, o gestionar y fortalecer la respuesta a una selección de actos de TIC maliciosos y, por extensión, reforzar la resiliencia cibernética nacional en general.

Es importante recordar no solo que estos son ejemplos ilustrativos, sino que los elementos importantes de la preparación y madurez cibernética nacional pueden no estar directamente asociados con el Marco y, por lo tanto, no se han incluido en la lista anterior. Sin embargo, el propósito de este informe es demostrar, como complemento, la evaluación más holística de la implementación nacional del Marco presentada en la Parte I de este estudio[12] — cómo un enfoque más centrado basado en perfiles de amenazas específicas puede agregar una capa adicional de análisis que puede refinar aún más la comprensión de un Estado de sus capacidades cibernéticas actuales.

En el preámbulo del Capítulo 4, se señala cómo, independientemente del perfil de amenaza, ciertas normas y capacidades fundamentales asociadas deben considerarse relevantes y aplicables sin

12 Refiérase a Samuele Dominioni y Giacomo Persi Paoli. 2023. Descubrir las necesidades de desarrollo de capacidades cibernéticas: Parte I. Clasificación de capacidades cibernéticas fundamentales. UNIDIR.

importar el escenario o la amenaza bajo consideración. Esto se refiere a la Norma A sobre cooperación interestatal y la Norma E sobre derechos humanos. El análisis de los tres escenarios se basa en este punto e identifica FCC específicas adicionales que parecen ser recurrentes en múltiples amenazas y en múltiples normas.

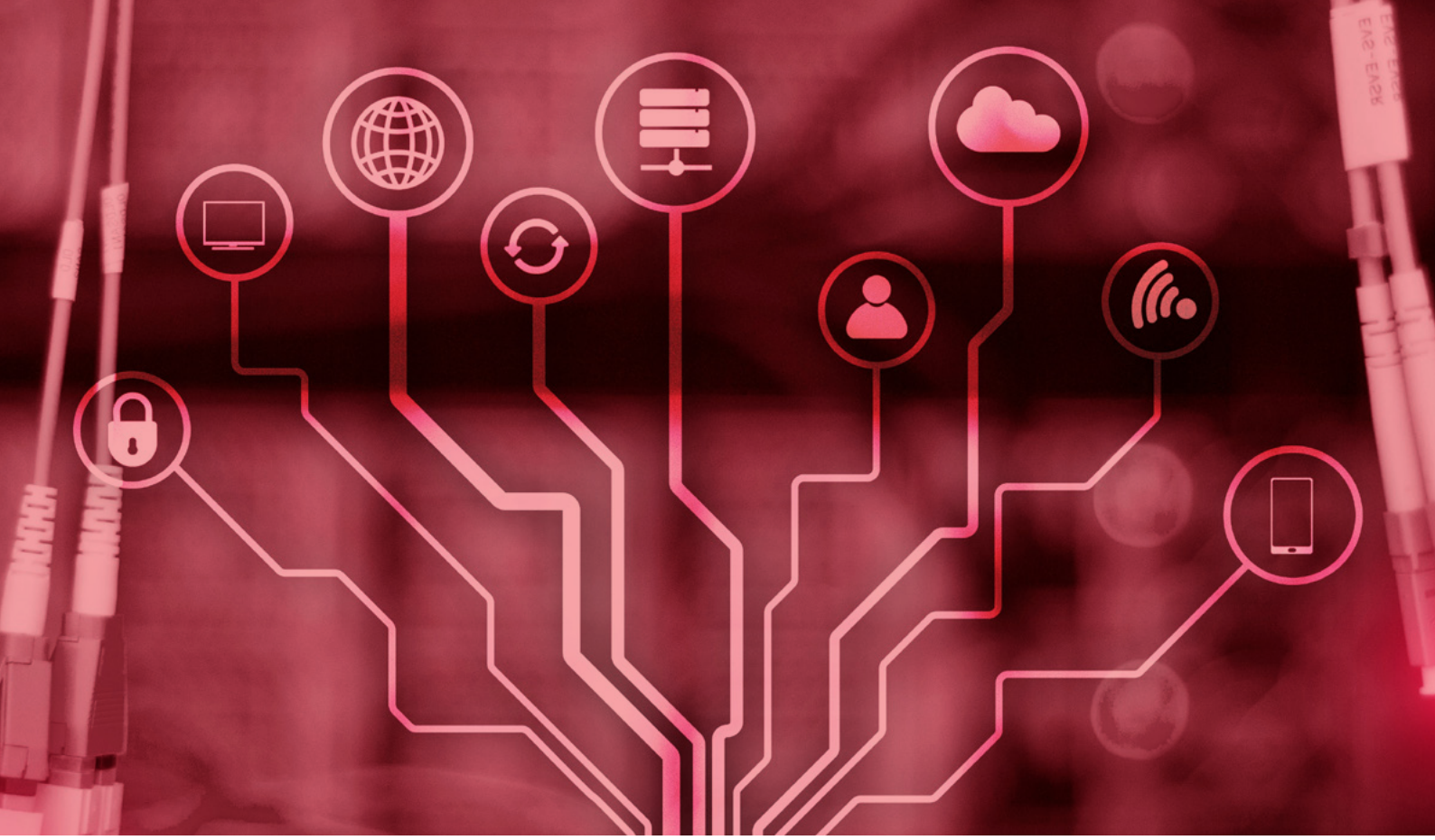
Desde una perspectiva de política y regulación, los Estados deben priorizar el desarrollo (y la revisión periódica) de estrategias y políticas nacionales integrales de seguridad cibernética que, en combinación con leyes adecuadas, permitan a los Estados tomar todas las medidas necesarias a nivel nacional e internacional para garantizar la protección del dominio de las TIC, incluso a través de cooperación de múltiples partes interesadas. Además, los Estados deben priorizar el desarrollo de posiciones integrales y públicas sobre cómo se aplica el derecho internacional al dominio de las TIC.

Desde una perspectiva de proceso, los Estados deben priorizar el desarrollo de mecanismos para facilitar la cooperación en asuntos relacionados con la seguridad de las TIC con todas las partes interesadas nacionales relevantes, incluidas las agencias gubernamentales, el sector privado y la comunidad técnica, y la sociedad civil, según corresponda. Esto garantizaría no solo flujos de información oportunos, eficientes y efectivos en tiempos de crisis, sino también acceso a activos de conocimiento que pueden aprovecharse según corresponda para compensar la posible escasez de experiencia disponible en el sector público. De manera similar, los Estados deben desarrollar mecanismos para facilitar la cooperación y el intercambio de información a nivel bilateral, regional e internacional. El desarrollo de procesos y mecanismos específicos permitiría la creación de **alianzas y redes que funcionan**.

En relación con las estructuras, los Estados deberían priorizar el desarrollo y la sostenibilidad de **capacidades de respuesta a incidentes informáticos** nacionales totalmente operativos que son elementos insustituibles de la primera línea de defensa contra actos maliciosos a las TIC. Se podrían explorar diversos acuerdos a nivel nacional y regional entre CSIRT/CERT públicos y privados para dar cuenta de las limitaciones en recursos, habilidades o tecnologías. Además, los Estados deberían priorizar la identificación de **dependencias responsables** dentro del gobierno nacional para actuar como **puntos focales para temas de TIC a nivel político y técnico,** incluso con la creación de un Punto de Contacto Nacional dedicado. La presencia de una **dependencia con la autoridad y los poderes para investigar y enjuiciar** actos maliciosos relacionados con las TIC parece ser un requisito transversal.

Si bien todos los sectores sufren una escasez de habilidades cibernéticas, la implementación exitosa del Marco se basará en la capacidad de los Estados para desarrollar internamente, o acceder a través de asociaciones externas, **conocimientos técnicos y jurídicos adecuados** para poder gestionar de manera efectiva los incidentes de TIC a nivel nacional y garantizar el cumplimiento del Marco, pero también para comprometerse constructivamente con sus homólogos a nivel internacional en cuestiones relacionadas con la seguridad de las TIC. Esto también se convertirá en una demanda cada vez mayor para los diplomáticos, quienes deberían fortalecer su comprensión de los problemas de las TIC y contar con el apoyo de especialistas y asesores según sea necesario.

Finalmente, la implementación exitosa del Marco dependerá también de la capacidad de un Estado para acceder a un cierto número de **tecnologías y soluciones técnicas** ya sea desarrollándolas a nivel nacional o accediendo a ellas a través de asociaciones con otros (por ejemplo, acuerdos bilaterales o regionales con otros Estados, o asociaciones público-privadas). Estas soluciones tecnológicas incluyen, pero no se limitan, a **capacidades para prevenir, detectar e interrumpir diferentes tipos de ataques** (por ejemplo, plataformas de inteligencia de amenazas, sistemas de alerta temprana) y soluciones para aumentar la confidencialidad, integridad y disponibilidad de sistemas y datos (por ejemplo, centros de datos basados en la nube).



Anexo 1. Tabla de Capacidades Cibernéticas Fundamentales

Norma A

Los Estados deben cooperar en el desarrollo y la aplicación de medidas para aumentar la estabilidad y la seguridad en el uso de las TIC y para prevenir prácticas de TIC que se reconozcan como dañinas o que puedan plantear amenazas a la paz y la seguridad internacionales.

POLÍTICAS Y REGLAMENTOS	
i	Interpretación nacional de la norma.
ii	Política y estrategia de seguridad cibernética (y plan de implementación nacional), o legislación sobre seguridad cibernética nacional (preferiblemente con un enfoque pangubernamental).
iii	Enfoque de gestión de riesgos cibernéticos (que incluya las infraestructuras críticas).Política exterior que reconozca la ciberseguridad como una de las prioridades.
iv	Política exterior que reconozca la ciberseguridad como una de las prioridades.
v	Compromiso público con el Marco de Comportamiento Responsable de los Estados en el ciberespacio.
vi	Declaración pública sobre las capacidades cibernéticas nacionales disponibles (información no clasificada).
vii	Estrategias y planes nacionales para el desarrollo de competencias cibernéticas.
ESTRUCTURAS Y PROCESOS	
i	Centro nacional, agencia o entidad responsable de la ciberseguridad.
ii	Capacidades nacionales o regionales de detección y respuesta a incidentes cibernéticos (p. ej., CERT/CSIRT o un Centro de Operaciones de Seguridad).
iii	Punto de contacto (PoC) a nivel diplomático y técnico.
iv	Cooperación e intercambio de información entre la legislación y las fuerzas del orden.
v	Mecanismos de supervisión independientes y eficaces (judiciales, administrativos, parlamentarios) capaces de garantizar la transparencia y la rendición de cuentas en relación con el funcionamiento del Estado en el ámbito de las TIC.
ASOCIACIONES Y REDES	
i	Cooperación intrasectorial (sector privado, sociedad civil, comunidad técnica, academia).
ii	Cooperación intragubernamental (p. ej., reuniones interministeriales, grupos de trabajo).
iii	Cooperación bilateral, regional y multilateral en diferentes niveles (técnico, operativo, diplomático).
iv	Acuerdos multilaterales (p. ej., el Convenio de Budapest, el Convenio de Malabo).
PERSONAS Y HABILIDADES	
i	Capacidades diplomáticas para participar en procesos internacionales e intergubernamentales.
ii	Expertos y profesionales en políticas con conocimientos básicos de ciberseguridad.
iii	Expertos jurídicos con competencias jurídicas en derecho internacional relacionado con actividades en el ámbito de las TIC.
iv	Programas de “Formación de formadores” y certificación profesional.
v	Habilidades para gestionar incidentes de ciberseguridad, incluida la preparación, la respuesta y la recuperación, tanto a nivel nacional como internacional.
vi	Campañas sistemáticas de sensibilización, dirigidas al público en general, sobre la importancia de los parches de seguridad y otras prácticas básicas de higiene cibernética como las actualizaciones de software.
TECNOLOGÍA	
i	Capacidades para garantizar la ciberseguridad en los puntos finales (antivirus o actualizaciones y parches automáticos de productos digitales para mitigar errores de seguridad y vulnerabilidades).
ii	Capacidades técnicas para prevenir, detectar o interrumpir actos maliciosos relacionados con TIC.
iii	Soluciones técnicas para proteger las comunicaciones (p. ej., encriptación).

Norma B

En caso de incidentes de TIC, los Estados deben considerar toda la información relevante, incluidos el contexto más amplio del evento, las dificultades de la atribución en el entorno de las TIC y la naturaleza y el alcance de las consecuencias.

POLÍTICAS Y REGLAMENTOS	
i	Interpretación nacional de la norma.
ii	Posición(es) o declaración(es) nacional(es) sobre la aplicación del derecho internacional al uso de TIC por parte de los Estados.
iii	Clasificación (pública o no pública) de incidentes de TIC en términos de escala e impacto.
iv	Política (pública o no pública) de atribución que incluya definiciones, metodología y funciones y responsabilidades claras.
v	Reglamento que permita el intercambio de información con entidades comerciales relevantes y otras entidades no gubernamentales.
ESTRUCTURAS Y PROCESOS	
i	Criterios de prueba nacionales para determinar la atribución.
ii	Procesos y procedimientos que permitan el intercambio de información entre las entidades gubernamentales y no gubernamentales relevantes.
ASOCIACIONES Y REDES	
i	Cooperación entre las partes interesadas nacionales (p. ej., grupos de trabajo, plataformas de múltiples interesados.
ii	Cooperación bilateral y multilateral en temas de asistencia e intercambio de información a escala internacional.
iii	Cooperación bilateral y multilateral para la solución de diferencias y disputas a través de consultas y otros medios pacíficos.
PERSONAS Y HABILIDADES	
i	Habilidades para realizar (o evaluar, si la información es proporcionada por terceros) investigaciones técnicas de incidentes de TIC.
ii	Funcionarios públicos (incluido el personal diplomático) con las habilidades legales específicas en el contexto de las TIC, incluso sobre consultas y otros medios pacíficos para resolver disputas a escala internacional.
iii	Funcionarios públicos (incluido el personal diplomático) con habilidades de negociación y comunicación específicas para el contexto de las TIC.
TECNOLOGÍA	
i	Capacidades técnicas y forenses para investigar y determinar el origen de la actividad maliciosa relacionada con TIC.

Norma C

Los Estados no deben permitir a sabiendas que su territorio se utilice para cometer actos internacionalmente ilícitos utilizando TIC.

POLÍTICAS Y REGLAMENTOS	
i	Interpretación nacional de la norma, incluida la opinión del Estado sobre qué constituye un acto internacionalmente ilícito utilizando TIC.
ii	Estrategia y política de ciberseguridad, incluidas las disposiciones para prevenir, detectar e interrumpir el uso malicioso de TIC.
iii	Legislación específica que defina qué tipos de actividades de TIC están y no están permitidas en el territorio y que otorgue la autoridad para investigar, terminar o procesar judicialmente esos tipos de actividades.
ESTRUCTURAS Y PROCESOS	
i	Capacidades nacionales o regionales de detección y respuesta a incidentes cibernéticos (p. ej., CERT/CSIRT o un Centro de Operaciones de Seguridad).
ii	Capacidad de aplicación de la ley cibernética.
iii	Procedimiento para intercambiar información entre las partes interesadas nacionales pertinentes, incluidas las entidades no gubernamentales.
iv	Mecanismos para enviar o responder a solicitudes de asistencia (incluidos los procedimientos para evaluar las solicitudes).
ASOCIACIONES Y REDES	
i	Cooperación entre las partes interesadas nacionales pertinentes (p. ej., grupos de trabajo, plataformas de múltiples interesados) incluidas las asociaciones público-privadas relevantes.
ii	Acuerdos bilaterales y multilaterales en temas de asistencia e intercambio de información.
iii	Marco para el intercambio de información a nivel técnico (como la red FIRST).
PERSONAS Y HABILIDADES	
i	Capacidad para identificar e interrumpir actos maliciosos que utilicen TIC originados en el territorio propio.
ii	Funcionarios públicos (incluido el personal diplomático) con habilidades de comunicación específicas para el contexto de las TIC.
TECNOLOGÍA	
i	Capacidad técnica para prevenir, detectar o interrumpir actos maliciosos relacionados con TIC originados en el territorio propio.

Norma D

Los Estados deben considerar cuál es la mejor manera de cooperar para intercambiar información, ayudarse mutuamente, procesar judicialmente el uso terrorista y delictivo de TIC e implementar otras medidas de cooperación para hacer frente a este tipo de amenazas.

POLÍTICAS Y REGLAMENTOS	
i	Interpretación nacional de la norma.
ii	Firma y ratificación de instrumentos bilaterales, regionales o multilaterales en materia de ciberdelincuencia.
iii	Políticas que describan los mecanismos o procedimientos de cooperación e intercambio de información, que deben incluir a las entidades comerciales y otras entidades relevantes no gubernamentales.
iv	Legislación sobre ciberdelincuencia que garantice un enfoque tecnológicamente neutral.
ESTRUCTURAS Y PROCESOS	
i	Mecanismo para enviar o responder a solicitudes de asistencia (por ejemplo, solicitudes de asistencia jurídica mutua).
ii	Protocolos y procedimientos para recolectar, manipular y almacenar las pruebas digitales.
iii	Capacidad de aplicación de la ley cibernética.
iv	Capacidades nacionales o regionales de detección y respuesta a incidentes cibernéticos (p. ej., CERT/CSIRT o un Centro de Operaciones de Seguridad).
ASOCIACIONES Y REDES	
i	Cooperación bilateral, regional y multilateral para la investigación, la asistencia, la aplicación de la ley y el intercambio de información sobre el uso delictivo y terrorista de TIC (p. ej., tratados de asistencia jurídica mutua).
ii	Redes operativas (p. ej., INTERPOL I-24/7) y técnicas (p. ej., FIRST).
iii	Cooperación entre las partes interesadas nacionales pertinentes (p. ej., grupos de trabajo, plataformas de múltiples interesados), incluso a través de asociaciones público-privadas estructuradas.
PERSONAS Y HABILIDADES	
i	Capacidad para manejar la evidencia digital a nivel técnico y legal.
ii	Conocimiento de la legislación sobre ciberdelincuencia y terrorismo en otros Estados miembros.
iii	Capacidad para establecer relaciones con homólogos y socios bilaterales, regionales e internacionales para asegurarse de que las intervenciones sean eficientes y oportunas.
TECNOLOGÍA	
i	Capacidad técnica para prevenir, detectar o interrumpir actos maliciosos relacionados con TIC por parte de criminales y terroristas.
ii	Canales de comunicación o plataformas seguras para compartir información.

Norma E

Los Estados, al garantizar el uso seguro de las TIC, deben garantizar el pleno respeto de los derechos humanos, incluido el derecho a la libertad de expresión.

POLÍTICAS Y REGLAMENTOS	
i	Posición nacional sobre cómo se aplica el derecho internacional, incluido el derecho internacional de los derechos humanos.
ii	Políticas y estrategias de ciberseguridad coherentes con el derecho internacional de los derechos humanos (p. ej., la orientación presente en las resoluciones 68/167 y 69/166).
iii	No imponer restricciones indebidas a la libertad de expresión y la libertad de buscar, recibir y difundir información.
iv	Reglamentos, incluso para las empresas, concernientes al respeto de los derechos humanos en el diseño, el desarrollo y el uso de nuevas tecnologías.
v	Legislación en materia de vigilancia e interceptación por parte del Estado, de conformidad con el derecho a la privacidad.
vi	Leyes de protección de datos.
ESTRUCTURAS Y PROCESOS	
i	Mecanismos nacionales o regionales de supervisión que sean independientes y eficaces (judiciales, administrativos o parlamentarios) capaces de garantizar la transparencia y la rendición de cuentas en relación con la vigilancia de las comunicaciones, la intercepción y la recopilación de datos personales por parte del Estado.
ASOCIACIONES Y REDES	
i	Participar y consultar con las partes interesadas que abogan, promueven y analizan los derechos humanos y las libertades fundamentales en línea para comprender y minimizar los posibles impactos negativos de las políticas en las personas.
PERSONAS Y HABILIDADES	
i	Funcionarios públicos (incluidos quienes trabajan en las fuerzas del orden) con conocimiento de los derechos humanos en el ámbito digital, así como de cómo implementar los instrumentos internacionales de manera coherente con los derechos humanos.
ii	Conocimientos especializados localizados y contextualizados sobre derechos humanos., incluido el ámbito legal.
TECNOLOGÍA	
i	Capacidad tecnológica para garantizar el respeto a los derechos humanos en el uso de TIC por parte de actores estatales y no estatales.

Norma F

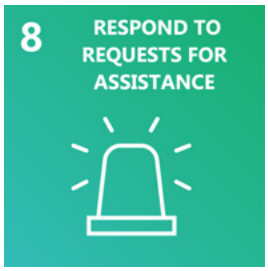
Un Estado no debe realizar ni apoyar a sabiendas una actividad con TIC contraria a sus obligaciones en virtud del derecho internacional que dañe o perjudique intencionalmente la infraestructura crítica.

POLÍTICAS Y REGLAMENTOS	
i	Posición nacional sobre la aplicabilidad del derecho internacional en el uso de TIC por parte de los Estados.
ii	Interpretación nacional de la norma.
iii	Clasificación (pública o no pública) de incidentes de TIC en términos de escala y gravedad.
iv	Concepción nacional de la infraestructura crítica.
ESTRUCTURAS Y PROCESOS	
i	Mecanismos nacionales o regionales de supervisión que sean independientes y eficaces (judiciales, administrativos, parlamentarios) capaces de garantizar la transparencia, según corresponda.
ASOCIACIONES Y REDES	
i	Marcos de cooperación bilateral, regional y multilateral para la cooperación y el intercambio de información.
PERSONAS Y HABILIDADES	
i	Conocimientos especializados de derecho internacional específicamente aplicables a las actividades realizadas en el ámbito de las TIC.
TECNOLOGÍA	
N/A	

Norma G

Los Estados deben tomar las medidas apropiadas para proteger su infraestructura crítica ante amenazas relacionadas con TIC.

POLÍTICAS Y REGLAMENTOS	
i	Interpretación nacional de la norma.
ii	Designación nacional de los sectores de infraestructura crítica.
iii	Clasificación (pública o no pública) de incidentes de TIC en términos de escala y gravedad.
iv	Legislación para la protección de la infraestructura crítica (que establezca normas, informes, auditorías, etc.).
v	Estrategia y política de ciberseguridad que incluya disposiciones sobre reducción del riesgo cibernético en la infraestructura crítica y medidas de ciberseguridad para productos de TIC, y que tenga en cuenta la resolución 58/199 sobre la cultura global de ciberseguridad y la protección de las infraestructuras críticas de información.
vi	Reglamento que permita el intercambio de información con entidades comerciales relevantes y otras entidades no gubernamentales.
ESTRUCTURAS Y PROCESOS	
i	Centro(s) nacional(es) u organismo(s) responsable(s) de la infraestructura crítica.
ii	Capacidades nacionales o regionales de detección y respuesta a incidentes cibernéticos (p. ej., CERT/CSIRT o un Centro de Operaciones de Seguridad).
iii	Mecanismos para el cumplimiento de las medidas de ciberseguridad en la infraestructura crítica.
iv	Planes de contingencia en caso de incidentes de TIC que involucren infraestructura crítica.
v	Procesos y procedimientos que permitan el intercambio de información entre las entidades gubernamentales y no gubernamentales relevantes.
ASOCIACIONES Y REDES	
i	Cooperación transfronteriza con los operadores y propietarios de infraestructura relevante (p. ej. coordinar las respuestas a incidentes, compartir buenas prácticas de protección de infraestructuras críticas).
ii	Cooperación entre las partes interesadas nacionales pertinentes (p. ej., comités interinstitucionales, plataformas de múltiples interesados) que incluyan las asociaciones público-privadas y los propietarios, operadores o administradores de infraestructura crítica.
PERSONAS Y HABILIDADES	
i	Habilidades técnicas para proteger la infraestructura crítica nacional contra actos maliciosos que involucren TIC.
ii	Entrenamientos y ejercicios dirigidos a mejorar las capacidades de respuesta y poner a prueba la continuidad de los servicios y los planes de contingencia ante ataques a la infraestructura crítica y que alienten a las partes interesadas a participar en actividades similares.
iii	Personal diplomático con la capacidad de **interactuar significativamente con sus homólogos en el tema específico de la infraestructura crítica**, en particular si la infraestructura es transnacional.
TECNOLOGÍA	
i	Capacidad técnica para prevenir, detectar o interrumpir actos maliciosos contra infraestructura crítica relacionados con TIC.



Norma H

Los Estados deben responder a las solicitudes apropiadas de asistencia de otro Estado cuya infraestructura crítica esté sometida a actos maliciosos con TIC.

POLÍTICAS Y REGLAMENTOS	
i	Interpretación nacional de la norma.
ii	Legislación que proporcione un marco para solicitar y brindar asistencia internacional.
iii	Estrategias y políticas de ciberseguridad que describan los mecanismos, procedimientos y procesos para responder a las solicitudes de asistencia.
ESTRUCTURAS Y PROCESOS	
i	Mecanismos eficientes para recibir, procesar, evaluar y responder solicitudes de asistencia, así como para prepararlas y enviarlas.
ii	Capacidad de aplicación de la ley cibernética.
ASOCIACIONES Y REDES	
i	Cooperación bilateral, regional y multilateral para la protección de infraestructura crítica (p. ej., creación de plantillas comunes para solicitar asistencia, firma de Memorandos de Entendimiento, etc.).
ii	Cooperación transfronteriza con los propietarios y operadores de infraestructuras importantes, así como con proveedores (p. ej., coordinación de sistemas de alerta de emergencia y de intercambio y análisis de información sobre vulnerabilidades).
iii	Cooperación entre las partes interesadas pertinentes (p. ej. asociaciones público-privadas y comités interinstitucionales).
PERSONAS Y HABILIDADES	
i	Capacidad para proporcionar asistencia transfronteriza eficaz y oportuna a los Estados que estén siendo objeto de ataques contra infraestructura crítica.
ii	Habilidades para atender y gestionar solicitudes de asistencia.
TECNOLOGÍA	
i	Capacidad técnica para prevenir, detectar o interrumpir actos maliciosos contra infraestructura crítica relacionados con TIC.
ii	Canales de comunicación o plataformas seguras para el intercambio de información relacionada con actos maliciosos contra infraestructuras críticas que involucren TIC.

Norma I

Los Estados deben tomar las medidas razonables para garantizar la integridad de la cadena de suministro y tratar de prevenir la proliferación de herramientas y técnicas de TIC maliciosas y el uso de funciones dañinas ocultas.

POLÍTICAS Y REGLAMENTOS	
i	Interpretación nacional de la norma.
ii	Leyes y reglamentos que prohíban la introducción de funciones ocultas dañinas y la explotación de vulnerabilidades en productos de TIC.
iii	Política y estrategia de ciberseguridad que abarque la seguridad de la cadena de suministro y describa los hitos importantes.
iv	Obligación de implementar reglas y estándares comunes interoperables a nivel mundial para la seguridad de la cadena de suministro (p. ej., ISO/IEC 20243).
v	Obligar a los proveedores a incorporar la seguridad y la protección en la gestión del ciclo de vida de sus productos de TIC.
ESTRUCTURAS Y PROCESOS	
i	Mecanismo de gobernanza de la gestión de riesgos en la cadena de suministro, lo cual debe incluir a los actores clave que representan los nodos de la cadena de valor.
ii	Mecanismo de evaluación y certificación de productos de TIC (nacional o en alianza con otros países).
iii	Acuerdos para garantizar la interoperabilidad de enfoques, métodos de certificación y certificaciones de productos de TIC entre las jurisdicciones.
ASOCIACIONES Y REDES	
i	Medidas de cooperación a nivel bilateral, regional y multilateral para, por ejemplo, intercambiar buenas prácticas de gestión de riesgos en la cadena de suministro o la certificación de productos de TIC.
PERSONAS Y HABILIDADES	
i	Capacidades en temas de seguridad y gestión de riesgos de la cadena de suministro.
ii	Habilidades de respuesta y gestión de incidentes.
iii	Personal diplomático capaz de interactuar significativamente con sus homólogos en **el tema específico de la seguridad de la cadena de suministro y los ataques a la cadena de suministro**.
TECNOLOGÍA	
i	Capacidad técnica para prevenir, detectar o interrumpir ataques a las cadenas de suministro.

Norma J

Los Estados deben alentar la notificación responsable de las vulnerabilidades de las TIC y compartir la información correspondiente sobre las soluciones disponibles para estas vulnerabilidades con el fin de limitar y posiblemente eliminar las amenazas potenciales a las TIC y la infraestructura dependiente de las TIC.

POLÍTICAS Y REGLAMENTOS	
i	Interpretación nacional de la norma.
ii	Medidas legales para frenar la distribución comercial de vulnerabilidades.
iii	Despenalización y protección legal para investigadores de seguridad y *hackers* éticos que deseen exponer vulnerabilidades.
iv	Política de divulgación coordinada de vulnerabilidades (CVD).
v	Marcos jurídicos que permitan la cooperación y el intercambio de información con vendedores y proveedores.
vi	Requisitos que debe cumplir una política y práctica de gestión de vulnerabilidades eficiente y eficaz.
ESTRUCTURAS Y PROCESOS	
i	Orientación sobre las respectivas funciones y responsabilidades de las diferentes partes interesadas en los procesos de notificación de vulnerabilidades, incluidos los tipos de información técnica que se debe divulgar y el manejo de datos confidenciales, etc.
ii	Protocolos establecidos para la comunicación e intercambio de información entre todos los interesados pertinentes (p. ej., gobiernos, proveedores y vendedores, investigadores de seguridad, equipos de respuesta a incidentes).
iii	Protocolos establecidos para la actualización y parcheo de los sistemas, en particular los relacionados con las infraestructuras dependientes de TIC.
iv	Orientación e incentivos para la divulgación coordinada de vulnerabilidades (p. ej., programas de recompensa por detección de fallos).
v	Campañas sistemáticas de concienciación (dirigidas tanto al público en general como al personal de industrias específicas, en particular aquellas que operen en sectores de infraestructura crítica) sobre la importancia de los parches de seguridad.
ASOCIACIONES Y REDES	
i	Cooperación bilateral, regional y multilateral para la divulgación de vulnerabilidades.
ii	Cooperación intersectorial con el sector privado, la sociedad civil y la comunidad técnica, incluidos vendedores y propietarios.
PERSONAS Y HABILIDADES	
i	Habilidades técnicas para identificar y resolver vulnerabilidades o gestionar la información relacionada con vulnerabilidades una vez recibida de terceros (p. ej., empresas que ofrecen recompensas por detección de fallos, investigadores de seguridad, proveedores).
ii	Habilidades necesarias de comunicación pública para enfrentar vulnerabilidades, especialmente cuando tienen impacto en la población general.
iii	Habilidades diplomáticas y de comunicación necesarias para poder participar exitosamente en las discusiones sobre gestión de vulnerabilidades con los actores estatales y no estatales pertinentes.
TECNOLOGÍA	
i	Capacidad técnica para identificar y resolver vulnerabilidades de TIC o para tomar medidas cuando la información sea proporcionada por terceros.
ii	Capacidad técnica para instalar parches a gran escala.

Norma K

Los Estados no deben realizar ni apoyar a sabiendas actividades que dañen los sistemas de información de los equipos autorizados de respuesta a emergencias (a veces conocidos como equipos de respuesta a emergencias informáticas o equipos de respuesta a incidentes de seguridad cibernética) de otro Estado. Un Estado no debe utilizar equipos autorizados de respuesta a emergencias para participar en actividades internacionales maliciosas.

POLÍTICAS Y REGLAMENTOS	
i	Posición nacional sobre la norma (o ciertos aspectos de ella).
ii	Declaración pública de que el Estado no utilizará los equipos autorizados de respuesta a emergencias para participar en actividades internacionales maliciosas u ofensivas y que respetará los principios éticos que orientan el trabajo de esos organismos.
iii	Lista de todos los CERT/CSIRT declarados.
iv	Política o estrategia de ciberseguridad que describa claramente la condición (p. ej., infraestructura crítica), la autoridad y los mandatos de los CERT/CSIRT, junto lo que distingue sus funciones únicas y neutrales de otras funciones gubernamentales.
v	Marco regulatorio del trabajo de los CERT/CSIRT alineado con las pautas y normas internacionales (p. ej., el código ético de FIRST o ISO 27/2001).
ESTRUCTURAS Y PROCESOS	
i	Capacidades nacionales o regionales de respuesta a incidentes cibernéticos (p. ej., CERT/CSIRT o un Centro de Operaciones de Seguridad).
ii	Mecanismos de supervisión independientes y eficaces (judiciales, administrativos, parlamentarios) capaces de garantizar la transparencia y la rendición de cuentas en relación con el funcionamiento del Estado en el ámbito de las TIC.
ASOCIACIONES Y REDES	
N/A	
PERSONAS Y HABILIDADES	
i	Habilidades para realizar (o evaluar, si la información es proporcionada por terceros) investigaciones técnicas sobre el uso indebido del CERT o CSIRT para realizar actividades maliciosas.
ii	Funcionarios públicos (incluidas las fuerzas armadas) conscientes de la función y la condición de los CERT/CSIRT.
iii	Conocimientos especializados de derecho internacional específicamente aplicables en el ámbito de las TIC.
TECNOLOGÍA	
N/A	

Derecho Internacional

Nota: esta sección de la tabla de FCC incluye elementos de derecho internacional adicionales que deben considerarse como complementarios o suplementarios a los específicamente incluidos en cada norma.

POLÍTICAS Y REGLAMENTOS	
i	Declaración pública de cómo entiende el Estado la aplicación del derecho internacional al ciberespacio.
ESTRUCTURAS Y PROCESOS	
i	Mecanismos de supervisión independientes (judiciales, administrativos, parlamentarios) capaces de garantizar la legalidad y la rendición de cuentas en relación con las operaciones del Estado en el ámbito de las TIC.
ASOCIACIONES Y REDES	
i	Cooperación con otros Estados miembros en las áreas de derecho internacional, legislación y políticas nacionales.
ii	Participación en los procesos multilaterales relacionados con el derecho internacional en el ámbito de las TIC.
PERSONAS Y HABILIDADES	
i	Conocimientos especializados de derecho internacional y las responsabilidades de los Estados en el ámbito cibernético.
ii	Capacidad para participar en discusiones regionales e internacionales sobre derecho internacional, incluida la capacidad de interactuar con la comunidad académica y la sociedad civil en general, en un idioma que podría no ser la lengua materna.
TECNOLOGÍA	
N/A	

Medidas de Fomento de la Confianza

POLÍTICAS Y REGLAMENTOS	
i	Divulgación pública de todas las estrategias, políticas y reglamentos nacionales relevantes de seguridad cibernética, idealmente con una traducción oficial al inglés (como mínimo) para facilitar el acceso a ellas y la transparencia.
ii	Identificar y considerar MFC apropiadas en sus contextos específicos y cooperar con otros Estados en su implementación.
ESTRUCTURAS Y PROCESOS	
i	Establecimiento de Puntos de Contacto (PoC) nacionales a nivel diplomático y técnico.
ii	Capacidades nacionales o regionales de respuesta a incidentes cibernéticos (p. ej., CERT/CSIRT o un Centro de Operaciones de Seguridad).
iii	Compartir información y buenas prácticas, lecciones o libros blancos sobre: • amenazas e incidentes existentes y emergentes relacionados con la seguridad de las TIC; • estrategias y normas nacionales para el análisis de vulnerabilidades en los productos de TIC; • enfoques nacionales y regionales para la gestión de riesgos y la prevención de conflictos.
iv	Intercambio de información sobre: • enfoques nacionales sobre la seguridad de las TIC; • protección de datos; • protección de la infraestructura crítica dependiente de TIC; • la misión y las funciones del organismo a cargo de la seguridad de las TIC, la estrategia de TIC a nivel nacional u organizacional, y los regímenes legales y de supervisión en cuyos marcos operan.
ASOCIACIONES Y REDES	
i	Participación en procesos de Naciones Unidas (p. ej., el GTCA).
ii	Participar en el diálogo a través de consultas bilaterales, subregionales, regionales y multilaterales.
iii	Participar en/con organismos regionales que desarrollan e implementan MFC.
iv	Participar en marcos de cooperación entre CERT/CSIRT u otros organismos técnicos de seguridad como la red FIRST u otros marcos regionales.
PERSONAS Y HABILIDADES	
i	Conocimiento de las MFC existentes y las maneras de activarlas o aprovecharlas en momentos de crisis.
ii	Conocimientos y competencias requeridos para actuar eficazmente como PoC nacional (si son designadas).
iii	Capacidad para hacer uso de las plataformas de intercambio de información existentes (p. ej., el portal de políticas cibernéticas de UNIDIR).
iv	Habilidades diplomáticas y de comunicación necesarias para participar eficazmente en debates sobre ciberseguridad con sus homólogos en otros países.
TECNOLOGÍA	
i	Canales y plataformas confiables de comunicación entre Estados.

@unidir
/unidir
/un_disarmresearch
/unidirgeneva
/unidir

Palais de Nations
1211 Geneva, Switzerland

WWW.UNIDIR.ORG