UNIDIR

¿Qué se necesita para crear capacidades cibernéticas?

Parte I. Clasificación de las Capacidades Cibernéticas Fundamentales

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.

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.

Sobre 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

Las denominaciones empleadas y la presentación del material en esta publicación no implican la expresión de ninguna opinión por parte de la Secretaría de las Naciones Unidas sobre la condición jurídica de ningún país, territorio, ciudad o zona o de sus autoridades, ni respecto de la delimitación de sus fronteras o límites. Las opiniones expresadas en esta publicación son responsabilidad exclusiva de los autores individuales. Y no reflejan necesariamente los puntos de vista ni las opiniones de las Naciones Unidas, UNIDIR, su personal o patrocinadores.

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

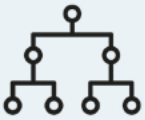
CBM	Medidas de fomento de la confianza
CERT/CSIRT	Equipo de respuesta a emergencias informáticas/Equipo de respuesta a incidentes de seguridad informática
DDOS	Denegación de servicio distribuida
FCC	Capacidades cibernéticas fundamentales
GEG	Grupo de Expertos Gubernamentales
TIC	Tecnologías de la información 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

En las últimas dos décadas los Estados han venido explorando activamente formas de garantizar la paz y la seguridad internacionales en el ámbito de las Tecnologías de la información y la comunicación (TIC). Estos esfuerzos dieron como resultado la adopción, por parte de la Asamblea General, de un conjunto de medidas conocidas colectivamente como el Marco de las Naciones Unidas para el comportamiento responsable de los Estados en el ciberespacio (en adelante, el Marco), que desarrolla qué deben y no deben hacer los Estados miembros en el entorno de las TIC desde una perspectiva de seguridad internacional. El Marco se basa en los componentes fundamentales de la creación de capacidades específicas: 11 normas voluntarias y no vinculantes de comportamiento estatal responsable, medidas de fomento de la confianza y el derecho internacional.

En el GTCA en curso (2021-2025) muchos Estados miembros han destacado la necesidad de apoyar la implementación del Marco a través de, entre otros aspectos, orientación, asistencia y esfuerzos dedicados a la creación de capacidades. Este informe es la primera parte de un estudio realizado por UNIDIR dirigido a apoyar a los Estados en sus esfuerzos por implementar el Marco y aumentar su ciberseguridad y su resiliencia.

En particular, este informe identifica las *capacidades cibernéticas fundamentales* (FCC), definidas como la combinación de políticas y reglamentos, procesos y estructuras, asociaciones y redes, personas y habilidades y las tecnologías que se **consideran necesarias** para implementar **cada elemento del Marco:** las 11 normas, el derecho internacional y las medidas de fomento de la confianza.

Políticas y Reglamentos 	Documentos oficiales relacionados con asuntos de ciberseguridad. Incluyen documentos que describan las posiciones, políticas y estrategias (desarrolladas específicamente para sectores clave, p. ej., infraestructura crítica, o para aplicaciones intersectoriales a escala nacional) de los Estados miembros, así como los marcos legales y regulatorios y las firmas de acuerdos u otros instrumentos de cooperación con partes interesadas internacionales.
Procesos y Estructuras 	Puestos clave, organismos o entidades responsables, otros mecanismos nacionales o regionales y procesos, procedimientos y protocolos oficiales relacionados con la ciberseguridad.
Asociaciones y Redes 	Iniciativas, tanto a nivel nacional como internacional, dirigidas a fortalecer las capacidades nacionales. A escala nacional incluyen mecanismos o instrumentos de cooperación intrasectorial e intragubernamental. A escala internacional, mecanismos o instrumentos de cooperación bilateral, regional y multilateral.
Personas y Habilidades 	Conocimientos y experiencia especializada en relación con la ciberseguridad. Cabe señalar que ciertos FCC incluidos en el pilar “personas y habilidades” también podrían satisfacerse mediante tercerización y el establecimiento de acuerdos con proveedores externos u otras partes interesadas cuando el Estado no pueda desarrollar o mantener internamente las capacidades especiales.
Tecnología 	Soluciones y capacidades técnicas a escala nacional relacionadas con la ciberseguridad. Cabe señalar que los FCC incluidos en el pilar “tecnología” también podrían satisfacerse mediante tercerización o proveedores externos de servicios a través de, por ejemplo, asociaciones público-privadas.

Es importante tener en cuenta que el propósito de los FCC es que actúen como las condiciones iniciales a partir de las cuales se podrían desarrollar respuestas más refinadas y completas una vez que se cumplan esas condiciones iniciales. Por lo tanto, las FCC representan los requisitos de

capacidad “mínimos” necesarios para la implementación del Marco, y no las mejores soluciones o los requisitos de capacidad “óptimos”.

Se puede utilizar el conjunto de FCC como una herramienta que permita identificar mejor los requisitos y la priorización de las intervenciones de creación de capacidades en función de las necesidades y los contextos nacionales específicos, reforzando así los vínculos entre la implementación del Marco y las discusiones relacionadas con la creación de capacidades, incluidas las que tengan lugar en el GTCA actual (y los potenciales Programas de Acción futuros).

1. Introducción

El área de las tecnologías de la información y la comunicación (TIC) ha cambiado y evolucionado a lo largo de décadas, y se ha expandido hasta abarcar casi todas las diferentes facetas de actividad humana. Naciones Unidas ha reconocido que hoy en día las TIC "tienen implicaciones para [...] la paz y la seguridad, los derechos humanos y el desarrollo sostenible. Las TIC y la conectividad global han sido un catalizador del progreso y el desarrollo humano al transformar las sociedades y economías y al ampliar las oportunidades de cooperación".[1] Junto con la creciente relevancia de las TIC en diferentes sectores, en las últimas décadas también se han realizado múltiples esfuerzos por establecer marcos regulatorios para las TIC.

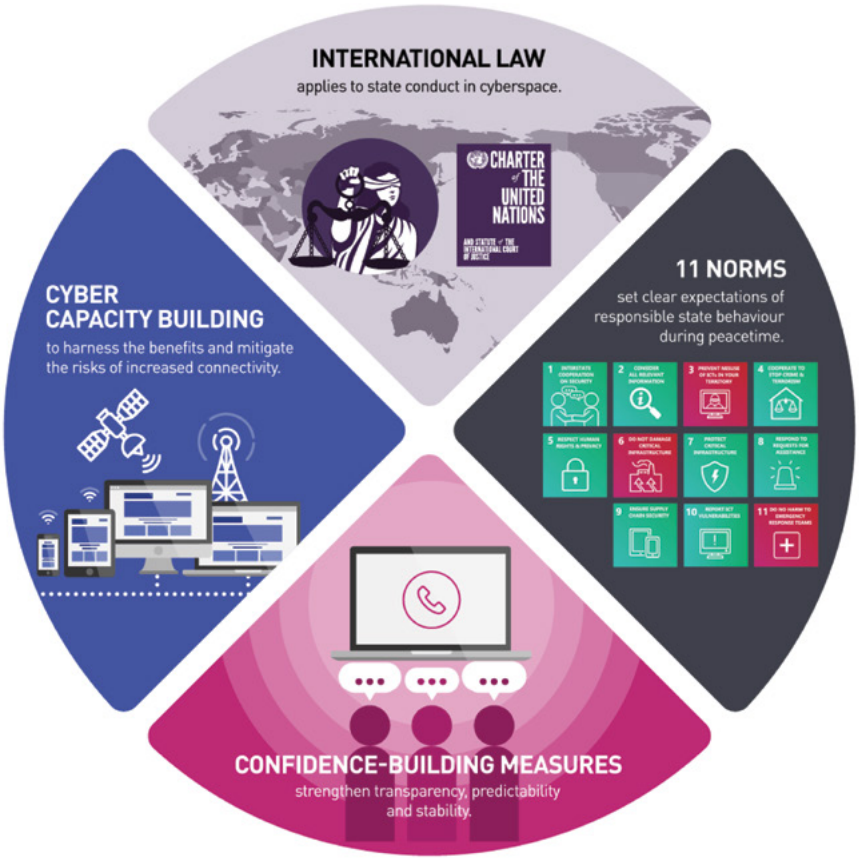
Entre estos esfuerzos por regular el campo de las TIC está el Marco para el comportamiento responsable de los Estados (en adelante, el Marco), que desarrolla qué deben y no deben hacer los Estados miembros en el entorno de las TIC desde una perspectiva de seguridad internacional. El Marco es el resultado de alrededor de dos décadas de negociaciones (en diferentes formatos) en las Naciones Unidas. En particular, se basa en el informe del Grupo de trabajo de composición abierta (GTCA) de 2021 sobre los desarrollos en el campo de las TIC en el contexto de la seguridad internacional y en los informes de consenso de los Grupos de Expertos Gubernamentales (GEG) de 2010, 2013, 2015 y 2021.

---

1 **OEWG. 2021. Final Substantive Report**, parágrafo 2.

En estos informes, que son de naturaleza acumulativa, los Estados miembros desarrollaron 11 normas voluntarias no vinculantes relacionadas con el comportamiento responsable de los Estados, recomendaron medidas específicas para el fomento de la confianza, la creación de capacidades y la cooperación, y determinaron que el derecho internacional, en particular la Carta de las Naciones Unidas Naciones, es aplicable y esencial para mantener la paz, la seguridad y la estabilidad en el entorno de las TIC. Estos tres elementos (normas, derecho internacional y medidas de fomento de la confianza), apoyados en la creación de capacidades, constituyen el Marco (ver la Figura 1).

Figura 1. 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

En el GTCA en curso (2021-2025) muchos Estados miembros han destacado la necesidad de apoyar la implementación del Marco a través de, entre otros aspectos, orientación, asistencia y esfuerzos dedicados a la creación de capacidades. En respuesta a esta demanda y con el fin de aumentar la ciberseguridad y la resiliencia de los Estados miembros, UNIDIR llevó a cabo una investigación con tres objetivos principales:

1. Identificar las capacidades cibernéticas fundamentales (FCC) que se consideran necesarias para implementar el Marco de manera eficaz.
2. Fortalecer los vínculos entre el Marco y la capacidad de los Estados para prevenir o mitigar eficazmente el impacto de determinadas actividades maliciosas de TIC.

3. Diseñar una herramienta que permita identificar mejor los requisitos y priorizar las intervenciones de creación de capacidades en función de las necesidades y los contextos nacionales específicos, reforzando así los vínculos entre la implementación del Marco y las discusiones relacionadas con la creación de capacidades, incluidas las que tengan lugar en el GTCA actual (y los potenciales Programas de Acción futuros).

El presente informe se centra en el objetivo 1, contribuye al objetivo 3 y aporta la base para abordar el objetivo 2, objeto de una publicación independiente.[2]

Nota sobre la Metodología[3]

La investigación se realizó en dos fases con un enfoque de métodos mixtos. La primera se concentró en la identificación de las denominadas FCC, que se definen como la combinación de políticas y reglamentos, procesos y estructuras, asociaciones y redes, personas y habilidades, y las tecnologías que se consideran necesarias para implementar el Marco (véanse las definiciones en el capítulo 2). Esta fase implicó un análisis documental de todos los informes acordados en el primer GTCA (2021) y producidos por los Grupos de Expertos Gubernamentales en cibernética (2010, 2013, 2015 y 2021) y literatura adicional. Posteriormente se llevaron a cabo entrevistas estructuradas con diplomáticos y profesionales expertos en ciberseguridad de Estados miembros seleccionados y otras partes interesadas (incluidas la sociedad civil y el sector privado).[4] Se utilizaron la investigación documental y un conjunto de entrevistas preliminares para generar una lista inicial de FCC. Luego, la segunda fase de la investigación consistió en poner a prueba la lista de FCC con ciberamenazas específicas (*ransomware*, ataque distribuido de denegación de servicio (DDOS) y manipulación de cadenas de suministro);[5] para ello se realizaron dos talleres con escenarios basados en amenazas (uno interno y otro con expertos externos).[6] Los datos derivados de los dos talleres fueron agregados y analizados. UNIDIR presentó los resultados preliminares del proyecto de investigación en un evento paralelo a la cuarta sesión del GTCA en Nueva York (6 al 10 de marzo de 2023). Finalmente, para refinar los resultados se llevó a cabo una ronda final de consultas con expertos externos.

---

2 Ver Samuele Dominioni y Giacomo Persi Paoli. 2023. Unpacking Cyber Capacity-Building: Part II. Introducing a Threat-Based Approach. UNIDIR.

3 Agradecemos a los Estados Miembros y las organizaciones que participaron en el proyecto de investigación: Argentina, Australia, República Checa, Dinamarca, Estonia, Ghana, Israel, Italia, Kenia, Jamaica, Malasia, Mauricio, México, Países Bajos, Singapur y Reino Unido; y FIRST, Global Forum for Cyber Expertise, INTERPOL, International Chamber of Commerce, Royal United Services Institute, Kaspersky, Microsoft y la Escuela de Estudios Internacionales de Rajaratnam (RSIS).

4 Se tomó en consideración la diversidad geográfica y de género al seleccionar las personas entrevistadas.

5 La selección se hizo considerando las amenazas que se mencionan frecuentemente en discusiones multilaterales.

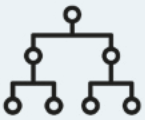
6 Se alternaron los talleres de expertos externos e internos con sesiones plenarias y grupos de trabajo con el fin de analizar, con el apoyo de escenarios específicos, los tres estudios de caso con miras a asociar los elementos relevantes del Marco con FCC específicas y las necesidades pertinentes de creación de capacidades. Por ejemplo, utilizando ransomware como punto de entrada, los participantes en el taller analizaron el Marco para identificar las normas, las leyes internacionales o CBM relevantes que podrían aplicarse al escenario. Luego seleccionaron las FCC más adecuadas para enfrentar la amenaza.

2. Introducción a las Capacidades Cibernéticas Fundamentales

Las FCC se definen como la combinación de políticas y reglamentos, procesos y estructuras, asociaciones y redes, personas y habilidades, y las tecnologías que se consideran necesarias para implementar el Marco.

A los efectos de este estudio estos cinco pilares se definen de la siguiente manera:

Tabla 1. Los Cinco Pilares para la Implementación del Marco

Políticas y Reglamentos 	Documentos oficiales relacionados con asuntos de ciberseguridad. Incluyen documentos que describan las posiciones, políticas y estrategias (desarrolladas específicamente para sectores clave, p. ej., infraestructura crítica, o para aplicaciones intersectoriales a escala nacional) de los Estados miembros, así como los marcos legales y regulatorios y las firmas de acuerdos u otros instrumentos de cooperación con partes interesadas internacionales.
Procesos y Estructuras 	Puestos clave, organismos o entidades responsables, otros mecanismos nacionales o regionales y procesos, procedimientos y protocolos oficiales relacionados con la ciberseguridad.
Asociaciones y Redes 	Iniciativas, tanto a nivel nacional como internacional, dirigidas a fortalecer las capacidades nacionales. A escala nacional incluyen mecanismos o instrumentos de cooperación intrasectorial e intragubernamental. A escala internacional, mecanismos o instrumentos de cooperación bilateral, regional y multilateral.
Personas y Habilidades 	Conocimientos y experiencia especializada en relación con la ciberseguridad. Cabe señalar que ciertos FCC incluidos en el pilar “personas y habilidades” también podrían satisfacerse mediante tercerización y el establecimiento de acuerdos con proveedores externos u otras partes interesadas cuando el Estado no pueda desarrollar o mantener internamente las capacidades especiales.
Tecnología 	Soluciones y capacidades técnicas a escala nacional relacionadas con la ciberseguridad. Cabe señalar que los FCC incluidos en el pilar “tecnología” también podrían satisfacerse mediante tercerización o proveedores externos de servicios a través de, por ejemplo, asociaciones público-privadas.

Es importante destacar que el propósito de las FCC, desarrolladas mediante la metodología que describe el capítulo 1, es representar las capacidades fundamentales o necesarias para implementar el Marco. La lista de FCC no pretende ser representativa de las mejores prácticas o medidas deseables. Se han desarrollado con la idea de que actúen como las condiciones iniciales a partir de las cuales se podrían desarrollar respuestas más refinadas y completas una vez que se cumplan esas condiciones iniciales. Por lo tanto, las FCC representan los requisitos mínimos de capacidad necesarios para la implementación del Marco y no las soluciones óptimas o las respuestas ideales. Por esta razón no se incluyeron en la lista elementos que no surgieron como verdaderamente necesarios o fundacionales porque su carácter era más aspiracional, deseable o “avanzado”.

También es importante señalar que se hace más hincapié en cuál capacidad debe estar presente que en cómo desarrollarla, aspecto que se mantiene como prerrogativa de cada país. En este informe se dan algunos ejemplos del "cómo", pero solo con fines ilustrativos y de orientación.

Finalmente, el propósito de las FCC identificadas es guiar a los Estados miembros en su implementación del Marco y pueden considerarse elementos importantes, incluso necesarios, para alcanzar una mayor madurez en los acuerdos nacionales de ciberseguridad. Sin embargo, centrarse solo en el Marco no será suficiente para garantizar la exhaustividad de la preparación y la resiliencia cibernética. En este sentido, este estudio complementa –en lugar de repetir o reemplazar– los enfoques existentes diseñados con el propósito específico de evaluar la preparación o la madurez cibernética general de cada país.

El Anexo 1 ofrece una descripción general de las capacidades relacionadas con cada componente del Marco y los capítulos 3-5 los describen más pormenorizadamente.

3. Desglose de las FCC: Normas de Comportamiento Responsable de los Estados

Esta sección describe las capacidades cibernéticas fundamentales que se requieren para implementar las 11 normas no vinculantes de comportamiento responsable de los Estados en el ámbito de las TIC (ver Figura 3). El capítulo está estructurado de manera que cada norma pueda leerse de forma independiente en función de los intereses específicos de cada lector. Algunas FCC puede aparecer en múltiples normas, a veces como repeticiones exactas o con descripciones más matizadas, según la norma. Estas normas fueron acogidas por la Asamblea General de las Naciones Unidas mediante la adopción de la resolución 70/237 en diciembre de 2015. Esta resolución exhortó a los Estados miembros a guiarse por las 11 normas no vinculantes propuestas por el cuarto GEG. En 2021, el informe final del sexto GEG agregó información adicional sobre estas normas y reafirmó su valor para orientar el comportamiento responsable de los Estados en el ciberespacio. El informe sustantivo del primer GTCA de 2021 también reconoció y reafirmó las 11 normas no vinculantes.

Figura 2. Normas de Comportamiento Responsable de los Estados en el Ciberespacio

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

Cabe destacar que ciertas normas deben considerarse esenciales y transversales y, por lo tanto, aplicables en todos los escenarios y condición previa para la implementación de todas los demás. Este es el caso de la Norma A,[7] que enumera los requisitos generales que sustentan la cooperación interestatal, y de la Norma E,[8] que se centra en el respeto y la protección de los derechos humanos.

Además, ampliando lo que afirma el informe de 2021 del GTCA –"la creación de capacidades debe respetar los derechos humanos y las libertades fundamentales, ser inclusiva y sensible a cuestiones de género, universal y no discriminatoria"[9] – se recomienda que los Estados miembros, al implementar las capacidades que identifica el Marco, consideren las maneras en que estas capacidades podrían afectar de manera diferenciada las dimensiones de género, incluidas las brechas de género

7 "De conformidad con los propósitos de las Naciones Unidas, incluido el mantenimiento de la paz y la seguridad internacionales, 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".

8 "Los Estados, al garantizar el uso seguro de las TIC, deben respetar las resoluciones del Consejo de Derechos Humanos 20/8 y 26/13 relacionadas con la promoción, la protección y el disfrute de los derechos humanos en Internet, así como las resoluciones 68/167 y 69/ 166 de la Asamblea General sobre el derecho a la privacidad en la era digital, con el fin de garantizar el pleno respeto a los derechos humanos, incluido el derecho a la libertad de expresión".

9 OEWG. 2021. Final Substantive Report, párr. 56.

entre ciberprofesionales,[10] las respuestas legales con enfoque de género a incidentes cibernéticos[11] y los impactos de género de los incidentes maliciosos[12] y sus respuestas.[13] Por otra parte, en el GTCA actual un número cada vez mayor de Estados ha reconocido la importancia de aplicar una perspectiva de género en las discusiones, en particular promoviendo el intercambio sobre los impactos de género de los incidentes de TIC y reduciendo la brecha digital de género. En vista de este creciente interés, en el futuro podrían realizarse investigaciones para guiar la incorporación de la perspectiva de género en todos los componentes del marco de comportamiento responsable de los Estados.

10 Véase Katharine Millar, James Shires, Tatiana Tropina. 2021. Gender Approaches to Cybersecurity: Design, Defence and Response. UNIDIR.

11 Ibid.

12 Véase Deborah Brown y Allison Pytlak. 2020. Why Gender Matters in International Cyber Security. Women's International League for Peace and Freedom and the Association for Progressive Communications.

13 Sergio Droz. 2021. Diversity and Cyber Resilience: Views of an Incident Responder.

3.1 Norma A

De conformidad con los propósitos de las Naciones Unidas, incluido el mantenimiento de la paz y la seguridad internacionales, 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

En consideración del amplio espectro de acciones posibles que los Estados Miembros pueden tomar para implementar esta norma, se recomienda hacer **una interpretación nacional de la norma** antes de tomar cualquier otra acción. Al pensar detenidamente en cómo implementar esta norma a nivel nacional, los Estados miembros pueden reflexionar sobre cómo cooperar con otras partes interesadas para cumplir los objetivos que describe la norma. Posteriormente lo esencial sería la adopción de un **política, estrategia o legislación en materia de ciberseguridad** que describa los principios y los objetivos (y el plan de implementación pertinente).[14] Es particularmente importante que la política o estrategia contemple un enfoque pangubernamental, lo que implica la posibilidad de tomar medidas en todos los niveles de gobierno. Además, los Estados miembros deben definir un **enfoque de gestión del riesgo cibernético** (incluida la infraestructura crítica) que incluya la cooperación con otras partes interesadas. Para fomentar medidas de cooperación a escala internacional se recomiendan declaraciones públicas que reconozcan **la ciberseguridad como una de las prioridades de política exterior,** un **compromiso público con el Marco,** y cómo este se aplica al uso de las TIC por parte de los Estados. Una declaración pública sobre las **capacidades cibernéticas nacionales** también contribuiría a aumentar la transparencia[15] y, por tanto, la estabilidad y la paz. Finalmente, a la luz de todas las habilidades y conocimientos requeridos que se describen a continuación, también se recomienda a los Estados que desarrollen **estrategias y planes nacionales para el desarrollo de habilidades cibernéticas.**

Estructuras y Procesos

Los Estados miembros deben tener o establecer múltiples estructuras que aumenten la estabilidad y la seguridad en el uso de las TIC, ente ellas, como mínimo, **un centro nacional**

14 Para obtener orientación adicional sobre cómo desarrollar estrategias nacionales de ciberseguridad consulte la Guía para desarrollar una estrategia nacional de ciberseguridad, producida bajo la coordinación de la UIT con la participación de 18 socios de organizaciones internacionales, el sector privado, la sociedad civil y el mundo académico: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2021-ncs-guide.pdf.

15 Con este fin, los Estados miembros pueden hacer uso de plataformas relevantes como, por ejemplo, Cyber Policy Portal, Cybil, la plataforma CoE Octopus, etc.

o una agencia o entidad responsable que dirija todos los asuntos relacionados con ciberseguridad; esto es clave para garantizar la coordinación a escala nacional. A un nivel más operativo, las estructuras clave adicionales que los Estados miembros deben tener disponibles son: **capacidades nacionales o regionales de detección y respuesta a incidentes cibernéticos** (por ejemplo, CERT/CSIRT o Centros de Operaciones de Seguridad), así como **Puntos de contacto (PoC)** a nivel diplomático y técnico.[16] Los puntos de contacto pueden desempeñar un papel clave en la mejora de la comunicación entre los Estados miembros y contribuir así a la desescalada de posibles crisis en diversos ámbitos y generar confianza.[17] Considerando la naturaleza criminal de muchos incidentes cibernéticos, también debe contemplarse la **cooperación policial** (p. ej., estableciendo procedimientos para el intercambio de información). Para garantizar que se tomen todas las medidas conforme al Marco se debe establecer un **mecanismo de supervisión independiente y eficaz** (judicial, administrativo, parlamentario) capaz 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

Como describe el informe del GEG de 2021 la cooperación que abarca esta norma puede fomentarse en todos los niveles de gobernanza. Con este fin se deben considerar dos ejes principales de cooperación: nacional e internacional. Por un lado, para reducir los riesgos de trabajar en silos sería esencial desarrollar la **cooperación intrasectorial** (p. ej., con el sector privado, la sociedad civil y la academia) e **intragubernamental** (p. ej., reuniones interministeriales, grupos de trabajo). Por otro lado, es importante desarrollar **cooperación a nivel bilateral, regional y multilateral** en diferentes etapas (p. ej., técnicas, policiales, diplomáticas) y comprometerse con **instrumentos ya previstos en acuerdos multilaterales** (p. ej., el Convenio de Budapest sobre cibercriminalidad o el Convenio de Malabo para la protección de datos personales).[18]

Personas y Habilidades

En vista de la amplia gama de medidas que los Estados miembros pueden tomar para implementar la Norma A, la tabla de FCC identifica un conjunto amplio y básico de habilidades. Para los Estados miembros son importantes las **capacidades diplomáticas** para participar en procesos internacionales e intergubernamentales relacionados con la seguridad de las TIC. A la luz de esto, también resulta beneficioso que el personal diplomático cuente con **conocimientos básicos en ciberseguridad.** Para poder participar adecuadamente en los foros internacionales los Estados miembros

16 Cabe señalar que, al momento de redactar este documento, en el contexto del GTCA se ha debatido ampliamente el establecimiento de un directorio de PoC nacionales. Se espera que se tome una decisión formal sobre este punto durante la quinta sesión oficial del GTCA, prevista del 24 al 28 de julio de 2023. Si bien las negociaciones en curso se centran en un directorio de PoC a nivel estatal, también se ha propuesto y discutido la posibilidad de desarrollar un directorio ampliado que incluya a otras partes interesadas.

17 Samuele Dominioni. 2023. Operationalizing a Directory of Points of Contact for Cyber Confidence-Building Measures. UNIDIR.

18 Este informe reconoce las negociaciones en curso del Comité Ad Hoc para elaborar una convención internacional integral para contrarrestar el uso de las tecnologías de la información y la comunicación con fines delictivos.

también necesitan expertos jurídicos con **conocimiento de derecho internacional concerniente a actividades en el ámbito de las TIC.** Por otro lado, en cuanto al aspecto interno de las medidas para aumentar la estabilidad y la seguridad en el uso de las TIC por parte de los Estados, es importante establecer programas de **formación de formadores** con un amplio plan de estudios sobre habilidades relacionadas con la ciberseguridad (esto contribuiría asimismo a limitar las consecuencias de la escasez mundial de habilidades en ciberseguridad). Los Estados miembros también deberían tener **expertos e investigadores en ciberseguridad** capaces de realizar un seguimiento del panorama de amenazas y sus constantes cambios. Finalmente, para los objetivos de la norma también sería relevante realizar **campañas sistemáticas de sensibilización** relacionadas con la importancia de los parches de seguridad y otras prácticas básicas de "higiene cibernética" dirigidas al público en general.

Tecnología

Si bien la norma no implica el uso de tecnologías específicas, algunas tecnologías podrían considerarse importantes para apoyar la implementación de la norma. La tabla de FCC identifica **capacidades para garantizar la protección de los productos TIC** (como antivirus y actualizaciones y parches automáticos en productos digitales), **para prevenir, detectar e interrumpir actos maliciosos a través de TIC** (como herramientas para realizar pruebas de penetración) y **para proteger las comunicaciones** (por ejemplo, técnicas de cifrado).

3.2 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

La atribución es una actividad compleja. Por este motivo el desarrollo de una **interpretación nacional** de la norma es un elemento fundamental para su implementación. La interpretación abarcaría, por ejemplo, qué tipo(s) de atribución (técnica, legal o política)[19] está considerando el Estado y cómo los diferencia. Si bien los Estados podrían decidir hacer atribuciones políticas basándose exclusivamente en la atribución técnica, se recomienda que los Estados miembros publiquen **declaraciones (o posiciones) relativas a sus interpretaciones del derecho internacional** en materia de responsabilidad estatal en el contexto de las operaciones con TIC. Los Estados miembros deberían posteriormente desarrollar, e idealmente poner a disposición del público **clasificaciones de incidentes de TIC en términos de escala e impacto**. Esto ayudaría a aumentar la transparencia sobre qué tipo de incidentes malintencionados con TIC interpretaría un Estado miembro como un hecho internacionalmente ilícito. Es igualmente importante que los Estados miembros desarrollen políticas que describan la **metodología y la cadena de responsabilidad** del proceso de atribución; esto aportaría un marco útil y claro para la toma de decisiones relacionadas con la atribución y evitaría, por ejemplo, escenarios en los que un Estado miembro llevara a cabo procesos de atribución paralelos a través de diferentes órganos estatales sin coordinación central. En algunos casos, para llevar a cabo la atribución los Estados miembros podrían necesitar tener acceso a datos que están en poder de actores no estatales. Por lo tanto, se recomienda adoptar **reglamentos que establezcan medios para el intercambio de información** entre actores gubernamentales y no gubernamentales.

Estructuras y Procesos

En vista de la dificultad de identificar a los perpetradores responsables de un acto malicioso con TIC y evitar el riesgo de atribuirlo erróneamente, una vez que se ha evaluado que el acto malicioso violó los marcos legales o normativos, los Estados Miembros deben hacer la atribución con base en **normas adecuadas de prueba.**[20] Otro elemento importante para la implementación de la norma tiene que ver con

19 Véase Andraz Kastelic. 2021. Non-Escalatory Attribution of International Cyber Incidents Facts, International Law and Politics. UNIDIR.

20 Si bien es un asunto secundario al propósito de este estudio, debe destacarse que los estándares de prueba también pueden ser relevantes para establecer la responsabilidad penal individual y para enjuiciar el delito cibernético de manera más general.

los **procesos y procedimientos que permitan el intercambio de información** con actores estatales y no estatales (incluso para acceder a pruebas extraterritoriales), que podrían resultar cruciales para realizar atribuciones fundamentadas.

Asociaciones y Redes

Los actos maliciosos relacionados con TIC suelen tener una dimensión intersectorial/nacional. Por lo tanto, para realizar correctamente la atribución se recomienda la cooperación entre las partes interesadas nacionales e internacionales pertinentes. Para este fin, y en términos de cooperación interna, serviría establecer **grupos de trabajo o plataformas que reúnan a múltiples interesados**. Esto aumentaría el intercambio de información y reduciría el efecto de trabajar en silos. En cuanto a la cooperación internacional, es muy importante **fomentar la cooperación bilateral y multilateral en términos de asistencia e intercambio de información**. La cooperación a escala regional e internacional, incluida la cooperación entre los Equipos de Respuesta a Emergencias Informáticas (CERT), los Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT) nacionales, las autoridades de los Estados en materia de TIC y la comunidad de múltiples interesados, puede fortalecer la capacidad de los Estados para detectar e investigar incidentes maliciosos relacionados con TIC y fundamentar sus preocupaciones y hallazgos antes de llegar a una conclusión sobre un incidente. Ante los posibles aspectos jurídicos derivados de una atribución, es importante el establecimiento de **cooperación bilateral y multilateral para la solución de diferencias** y disputas a través de consultas y otros medios pacíficos.

Personas y Habilidades

Realizar una atribución fundamentada puede implicar habilidades tanto técnicas como jurídicas. En cuanto a las primeras, los Estados miembros deben disponer de **expertos que lleven a cabo la investigación técnica de los incidentes de TIC** (p. ej., análisis forense de TIC) o, en caso de que la investigación técnica sea realizada por un tercero, **expertos con la capacidad de evaluar su calidad**. En cuanto a las habilidades legales, los funcionarios públicos (incluido el personal diplomático) deben tener **conocimiento de las disposiciones legales** (a nivel nacional e internacional) **específicas en el contexto de las TIC** y de los instrumentos disponibles para resolver disputas sobre estos asuntos de manera pacífica, o bien debe asesorados sobre tales asuntos por asesores en derecho internacional en materia de ciberseguridad. En casos de disputa, los funcionarios públicos deben ser capacitados en **habilidades de negociación y comunicación** específicas para el contexto de las TIC.

Tecnología

Para respaldar las evaluaciones legales y proporcionar evidencia útil que sustente las decisiones políticas concernientes a la atribución, se requieren **capacidades técnicas y forenses** para investigar y determinar el origen de la actividad maliciosa relacionada con TIC.

3.3 Norma C

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

Políticas y Reglamentos

Se recomienda que los Estados miembros elaboren sus **interpretaciones nacionales de la norma**, incluidas sus opiniones sobre el contenido, el alcance y las condiciones de la norma (p. ej., qué constituye un hecho internacionalmente ilícito utilizando TIC). Con respecto a la implementación de la norma, y considerando la expectativa de que si un Estado tiene conocimiento, o es notificado de buena fe, de que un hecho internacionalmente ilícito que utiliza TIC tiene origen en su territorio, "tomará medidas razonables dentro de sus capacidades para poner fin a la actividad en curso en su territorio",[21] los Estados miembros deben tener una **estrategia o política de ciberseguridad** que establezca las disposiciones que les permitan tomar medidas (p. ej., detectar e interrumpir) ante un incidente malicioso que utilice TIC. Además, los Estados también deben desarrollar **legislación** que defina qué tipos de actividades de TIC están y no están permitidas en el territorio del Estado, y que otorgue la autoridad para investigar, terminar y procesar judicialmente esos tipos de actividades.

Estructuras y Procesos

Se necesitan estructuras y procesos apropiados que le permitan a un Estado tomar medidas cuando tenga conocimiento, o sea notificado de buena fe, de que un hecho internacional ilícito tiene origen en su territorio. Con este fin, contar con **capacidad nacional o regional de detección y respuesta a incidentes cibernéticos** (p. ej., un CERT/CSIRT o un Centro de Operaciones de Seguridad) y **capacidad de aplicación de la ley cibernética** (p. ej., una unidad de delitos cibernéticos en las fuerzas policiales) o una agencia equivalente con el poder de investigar y procesar judicialmente, ayudaría a los Estados miembros a enfrentar las amenazas a través de medios proporcionados, apropiados y eficaces de manera coherente con el derecho internacional y nacional. Además, considerando la naturaleza de los incidentes maliciosos con TIC, sería necesario establecer **procedimientos para compartir información** entre las partes interesadas nacionales relevantes (p. ej., memorandos de entendimiento que describan la cooperación entre las fuerzas del orden público y los proveedores de servicios de internet). La norma también destaca la necesidad de solicitar ayuda a otros Estados miembros. En este caso es importante establecer mecanismos para **enviar o responder a solicitudes de asistencia** (incluidos un PoC o entidad nacional designada para recibir solicitudes de asistencia y procedimientos para evaluar la idoneidad de estas solicitudes).

---

21 **GGE. 2021**, para. 30 (a).

Asociaciones y Redes

El establecimiento de procedimientos para el intercambio de información tanto a nivel nacional como internacional requiere que los Estados miembros establezcan mecanismos de cooperación. A nivel nacional esto puede realizarse estableciendo **grupos de trabajo conjuntos, plataformas de múltiples interesados** (con actores estatales y no estatales, incluidos los CERT/CSIRT nacionales) y/o **asociaciones público-privadas** en sectores clave. A nivel internacional puede incluir **acuerdos bilaterales o multilaterales de asistencia e intercambio de información** (p. ej., asistencia legal recíproca). También se recomienda unirse a los **marcos ya existentes de intercambio de información a nivel técnico** (p. ej., la red FIRST), que reúnen una gran variedad de conocimientos técnicos especializados y posibilidades de cooperación en todo el mundo.

Personas y Habilidades

La norma se refiere a los pasos razonables que el Estado debe dar para poner fin a actividades maliciosas. Por lo tanto, los Estados miembros deben tener acceso a **conocimientos técnicos especializados en ciberseguridad**, sean internos o externos, que les permitan identificar e interrumpir actos maliciosos con TIC originados en su territorio (p. ej., habilidades de seguridad de redes). Otro conjunto pertinente de habilidades concierne a las **comunicaciones específicas en el contexto de las TIC** que serían necesarias para gestionar la comunicación pública y confidencial después de un incidente; esto incluye al personal diplomático.

Tecnología

Las capacidades tecnológicas relacionadas con esta norma tienen que ver con la **identificación, detección e interrupción de actos maliciosos que utilicen TIC** originados en el territorio de los Estados miembros.

3.4 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. Es posible que los Estados deban considerar si es necesario desarrollar medidas nuevas en esta materia.

Políticas y Reglamentos

Esta norma se refiere a conceptos aún abiertos a interpretaciones (p. ej., el uso de TIC por parte de terroristas). Por este motivo una capacidad pertinente y esencial es publicar una **interpretación nacional de la norma** en la que los Estados miembros elaboren sus puntos de vista. También se recomienda **firmar y ratificar instrumentos bilaterales, regionales o multilaterales** en materia de ciberdelincuencia.[22] Estos instrumentos facilitan la cooperación oportuna y eficaz entre los Estados. Además, debido a la perspectiva operativa de la norma, es importante que los Estados miembros adopten **políticas que describan los mecanismos o procedimientos para cooperar**, especialmente para **intercambiar información**, incluso con el sector privado (p. ej., a través del código penal). Para cooperar de la mejor manera en estos campos se recomienda desarrollar **legislación sobre ciberdelincuencia** que garantice un enfoque tecnológicamente neutral.[23]

Estructuras y Procesos

En esta norma es muy importante el establecimiento de **mecanismos eficientes para el envío y respuesta de solicitudes de asistencia** (p. ej., solicitud de asistencia legal recíproca). Igualmente importante es elaborar correctamente **protocolos y procedimientos** que permitan el uso de pruebas digitales en los tribunales. Estos protocolos y procedimientos deben precisar las pautas para recolectar, manipular y almacenar apropiadamente las pruebas digitales. También es importante que los Estados miembros desarrollen y fortalezcan su **capacidad para aplicar el derecho cibernético** (p. ej., unidades de policía cibernética), de modo que puedan cooperar de manera eficaz a nivel operativo en la lucha contra el uso criminal y terrorista de TIC. Además, contar con capacidad nacional o regional de detección y respuesta a incidentes cibernéticos (p. ej., CERT/CSIRT o Centros de Operaciones de Seguridad) es clave para identificar, documentar y notificar actos maliciosos que utilicen TIC.

---

22 Si bien la definición de ciberdelincuencia puede variar en las diferentes legislaciones nacionales, para los fines de este estudio la definimos como delitos contra la integridad, la disponibilidad y la confidencialidad de los datos.

23 Adoptar un enfoque tecnológicamente neutral al redactar nuevos proyectos de ley o enmiendas legales en materia de TIC añade flexibilidad al envío y la recepción de solicitudes y permite mantenerse al día ante la velocidad de los desarrollos tecnológicos; véase Samuele Dominioni, 2021 Enhancing Cooperation to Address Criminal and Terrorist Use of ICTs Operationalizing Norms of Responsible State Behaviour in Cyberspace. UNIDIR.

Asociaciones y Redes

La norma se centra en la cooperación, que puede tener lugar en múltiples niveles. Los Estados miembros deben establecer o fortalecer **mecanismos bilaterales, regionales y multilaterales para cooperar** en la investigación y el procesamiento judicial de los delitos cibernéticos. En este contexto siguen siendo preponderantes los tratados de asistencia jurídica mutua. También son esenciales las **redes operativas y técnicas** entre, por ejemplo, fuerzas o cuerpos de seguridad (p. ej., INTERPOL I-24/7) y servicios de respuesta a incidentes (p. ej., FIRST), a través de las cuales los agentes pueden tener acceso rápido a recursos relevantes (p. ej., bases de datos). Finalmente, la **cooperación entre las partes interesadas nacionales**, incluido el sector privado (p. ej., asociaciones público-privadas), es importante para evitar trabajar en silos y fomentar así una cooperación más eficaz y coordinada con otros Estados miembros.

Personas y Habilidades

Para implementar adecuadamente la norma los Estados miembros deben capacitar a su personal en diferentes habilidades.[24] Se recomienda contar con **expertos en la manipulación de evidencia digital a nivel técnico y legal**. También es importante la capacitación en la redacción de solicitudes de asistencia jurídica mutua, el uso de otros instrumentos (como las órdenes de allanamiento específicas para pruebas digitales) o el almacenamiento e intercambio adecuado de datos durante las investigaciones de delitos cibernéticos. De lo contrario, es posible que los tribunales no permitan la confiscación de pruebas digitales ni las acepten. Los Estados miembros también deben tener personal que **conozca la legislación de ciberdelincuencia en otros Estados miembros.**[25] Por último, para mejorar la cooperación entre las partes interesadas es importante que el personal de los Estados miembros (p. ej., el personal diplomático) tenga la **capacidad de conectarse (incluso de manera informal) con sus pares bilaterales, regionales e internacionales** y otros socios con el fin de asegurarse de que las intervenciones sean eficientes y oportunas.

Tecnología

La tecnología necesaria para la implementación de la norma se divide en dos áreas principales. Por un lado, existen capacidades tecnológicas para **prevenir, detectar o interrumpir actos maliciosos con TIC** (p. ej., plataformas de inteligencia sobre amenazas).[26] Por otro lado, están aquellas capacidades relacionadas con **canales de comunicación** seguros o plataformas para compartir información (p. ej., software policial para para compartir datos).

---

24 En este contexto cabe destacar el Programa Global sobre Ciberdelincuencia liderado por ONUDD: **Global Programme on Cybercrime (unodc.org).**

25 Esto es especialmente importante para los Estados miembros que necesitan enviar una solicitud de asistencia a otro Estado; véase Samuele Dominioni, 2021 Enhancing Cooperation to Address Criminal and Terrorist Use of ICTs Operationalizing Norms of Responsible State Behaviour in Cyberspace. UNIDIR.

26 Una plataforma de inteligencia sobre amenazas (TIP, por sus siglas en inglés) es "una solución tecnológica que recopila, acumula y organiza datos de inteligencia sobre amenazas de múltiples fuentes y en múltiples formatos"; ver: "multiple sources and formats"; véase: **https://www.paloaltonetworks.com/cyberpedia/what-is-a-threat-intelligence-platform#:~:text=A%20Threat%20Intelligence%20Platform%20(TIP,threat%20identification%2C%20investigation%20and%20response.**

3.5 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 relacionadas con la promoción, la protección y el disfrute de los derechos humanos en Internet, así como las resoluciones 68/167 y 69/ 166 de la Asamblea General sobre el derecho a la privacidad en la era digital, con el fin de garantizar el pleno respeto a los derechos humanos, incluido el derecho a la libertad de expresión.

Políticas y Reglamentos

Esta es una de las normas generales que abarcan todas las capacidades de todos los componentes del marco. En consecuencia, para garantizar que su aplicación sea coherente los Estados miembros deben publicar una **posición nacional sobre cómo se aplica el derecho internacional, incluido el derecho internacional de los derechos humanos, en el ámbito de las TIC**. Por consiguiente, es fundamental que los Estados miembros **desarrollen 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). La norma también llama a no imponer restricciones indebidas a la libertad de expresión y la libertad de buscar, recibir y difundir información. En la mayoría de los casos esto se implementaría **absteniéndose de establecer ese tipo de restricciones** (p. ej., mediante la censura de sitios web). Por el contrario, los Estados miembros deben adoptar **reglamentos, incluso para las empresas, concernientes al respeto de los derechos humanos en el diseño, el desarrollo y el uso de nuevas tecnologías**. Además, se recomienda adoptar **legislación que establezca límites a la vigilancia e interceptación por parte del Estado**, de conformidad con el derecho a la privacidad. Por último, los Estados miembros deberían tener **leyes de protección de datos** que definan el marco jurídico para la manipulación de datos de las personas físicas.

Estructuras y Procesos

Los Estados miembros deben establecer **mecanismos nacionales o regionales de supervisión que sean independientes y eficaces** (p. ej., judiciales, administrativos o parlamentarios) capaces de garantizar la transparencia, la proporcionalidad y la rendición de cuentas en relación con la vigilancia de las comunicaciones, la intercepción y la recopilación de datos personales. Estos mecanismos pueden referirse a entidades específicas (ad hoc) o a otras ya existentes con la autoridad específica para garantizar los principios mencionados anteriormente (p. ej., un comité parlamentario).

Asociaciones y Redes

Las capas adicionales de entendimiento en el informe de 2021 del GEG reconocen que “una variedad de partes interesadas pueden contribuir de diferentes maneras a la protección y la promoción de los derechos humanos y las

libertades fundamentales en línea y fuera de línea".[27] En vista de esto, sería fundamental **participar y consultar con las partes interesadas** que abogan, promueven y analizan (p. ej. la academia) los derechos humanos y las libertades fundamentales en línea para comprender y minimizar los posibles impactos negativos de este tipo de políticas en las personas.

Personas y Habilidades

Dado el objetivo general de la norma y sus implicaciones concretas, es pertinente que los funcionarios públicos (incluidos quienes trabajan en las fuerzas del orden) tengan **conocimiento de los derechos humanos en el ámbito digital**,[28] así como de cómo **implementar los instrumentos internacionales** (p. ej., las solicitudes de asistencia jurídica mutua) de manera **coherente con los derechos humanos**. Por otra parte, es importante que los Estados miembros cuenten con **expertos en derechos humanos** con conocimientos especializados en sus contextos específicos.

Tecnología

Existen algunas **capacidades tecnológicas para garantizar el respeto a los derechos humanos** en el uso de TIC por parte de actores estatales y no estatales. Entre estas, las soluciones de ciberseguridad de punto final pueden proteger contra spyware, y el software de encriptación puede asegurar las comunicaciones.

---

27 **GGE. 2021,** para. 41.

28 Hay cursos disponibles, como un curso del Consejo de Europa sobre educación en derechos humanos para profesionales del derecho que se centra en los delitos cibernéticos y las pruebas electrónicas; ver: **https://www.coe.int/en/web/help/courses#{%2258133235%22:[9]}.**

3.6 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 intencionalmente la infraestructura crítica o perjudique de otro modo el uso y la operación de la infraestructura crítica necesaria para brindar servicios al público.

Políticas y Reglamentos

En vista del enfoque de la norma sobre las obligaciones de los Estados en el marco del derecho internacional, se recomienda que los Estados miembros elaboren y pongan a disposición del público sus **posiciones nacionales sobre cómo se aplica el derecho internacional** al uso de las TIC por parte de los Estados. Es importante que presenten sus **interpretaciones nacionales** del término "apoyar a sabiendas", sus clasificaciones de incidentes de TIC en términos de escala y gravedad (incluso con referencia a qué se entiende por "dañe" y "perjudique") y su **concepto de lo que constituye, en su contexto nacional, "infraestructura crítica".**[29] De esta forma los Estados miembros pueden precisar la infraestructura o los sectores relacionados que consideran críticos.

Estructuras y Procesos

Para asegurarse de cumplir el objetivo de la norma, los Estados miembros deberían establecer **mecanismos nacionales o regionales de supervisión que sean independientes, eficaces** (judiciales, administrativos, parlamentarios) y capaces de garantizar la transparencia en el comportamiento de los Estados (p. ej., un comité parlamentario).

Asociaciones y Redes

Dada la dimensión transnacional de la conducta de los Estados en el ámbito de las TIC, sería fundamental que los Estados miembros participaran en **marcos de cooperación bilateral, regional y multilateral** para el intercambio de información, incluso en cuanto a la interpretación nacional de la norma. Esto podría ayudar a aumentar la transparencia en torno a sus designaciones y sus métodos de categorización de infraestructura crítica, con el fin de ayudar a construir entendimientos comunes respecto de la protección de sectores considerados críticos.

Personas y Habilidades

Los funcionarios públicos deben tener **conocimientos jurídicos, incluido el derecho**

29 Por ejemplo, salud, energía, generación de energía, agua y saneamiento, educación, servicios comerciales y financieros, transporte, telecomunicaciones y procesos electorales, y la infraestructura esencial para la disponibilidad y la integridad general de internet; ver GTCA, 2021. Final Substantive Report, párr. 18

internacional y su aplicabilidad en el dominio de las TIC, para implementar la norma y sus capacidades fundamentales relacionadas (p. ej., la interpretación nacional de la norma).

Tecnología

Este estudio no identificó ninguna capacidad tecnológica fundamental necesaria para implementar esta norma.

3.7 Norma G

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

Políticas y Reglamentos

En primer lugar, sería importante que los Estados miembros elaboraran su **interpretación nacional de la norma** y, en ella, definieran su comprensión del término "apropiadas". Este documento también debería incluir cuáles **sectores de infraestructura crítica** consideran que deben ser protegidos, así como las **clasificaciones de incidentes de TIC, en términos de escala y gravedad**, específicos para sus infraestructuras críticas.[30] Para proteger la infraestructura crítica es fundamental que los Estados miembros adopten un **marco legislativo** idóneo para este propósito (p. ej., mediante el establecimiento de reglamentos sobre su construcción, incluidos los estándares mínimos de seguridad, los mecanismos de notificación y auditorías). Por otra parte, como establece la norma, los Estados miembros deben considerar, en sus políticas y estrategias de ciberseguridad, **la resolución 58/199 de la Asamblea General**[31] sobre la reducción de riesgos para las infraestructuras de información críticas. Finalmente, dado que en muchos países actores no estatales desempeñan una función importante en la gestión de la infraestructura crítica, sería importante establecer r**egulaciones sobre el intercambio de información entre los sectores público y privado.**

Estructuras y Procesos

En términos de estructuras, los Estados miembros deberían establecer **un centro nacional o una agencia responsable de la infraestructura crítica**, así como **capacidades nacionales o regionales de detección y respuesta a incidentes cibernéticos** (p. ej., CERT/CSIRT o Centros de Operaciones de Seguridad) que desempeñarían una función fundamental en la protección de las infraestructuras críticas. En cuanto a los procesos, es importante que los Estados Miembros establezcan e implementen **mecanismos diseñados para asegurar el cumplimiento** de las normas pertinentes y otros requisitos reglamentarios (p. ej., auditorías, pruebas de preparación y ejercicios basados en escenarios para probar la resistencia y eficacia de los mecanismos y procedimientos de respuesta a incidentes); también **planes de contingencia** en caso de que se produzcan incidentes con TIC que afecten la infraestructura crítica (incluidas

30 Los dos documentos pueden emitirse por separado.

31 Esta resolución, titulada "Creación de una cultura global de ciberseguridad y protección de las infraestructuras críticas de la información", establece 11 elementos para la protección de las infraestructuras de información críticas. La resolución también invita a los Estados miembros a tomar en consideración estos 11 elementos al desarrollar sus estrategias de reducción de riesgos para las infraestructuras de información críticas, de conformidad con las leyes y reglamentos nacionales. Para obtener más información, consulte **https://documents-dds-ny.un.org/doc/UNDOC/GEN/N03/506/52/PDF/N0350652.pdf?OpenElement**

medidas para restaurar la funcionalidad de la infraestructura crítica dañada). Por último, es necesario implementar p**rocesos y procedimientos que permitan el intercambio de información** entre las entidades gubernamentales y no gubernamentales que participan en el ecosistema de infraestructura crítica.

Asociaciones y Redes

Dada la dimensión transnacional de muchos de los incidentes que involucran TIC y de algunas infraestructuras críticas, se recomienda que los Estados miembros establezcan una **cooperación transfronteriza con las partes interesadas pertinentes** (p. ej., operadores y propietarios) para compartir información y buenas prácticas de protección de infraestructuras críticas y coordinar las respuestas. Esto podría incluir la participación de los Estados en iniciativas voluntarias para la planificación de la evaluación de riesgos y la continuidad de las operaciones (resiliencia, recuperación y contingencia) en las que participen otras partes interesadas y que tengan como objetivo mejorar la seguridad y la resiliencia de la infraestructura crítica que brinda servicios a nivel regional o internacional contra amenazas existentes y emergentes. Por otra parte, teniendo en cuenta el ecosistema multipartita de la infraestructura crítica, y con el fin de garantizar una protección coherente y completa, los Estados miembros deben establecer **mecanismos de cooperación entre las partes interesadas nacionales pertinentes** (p. ej., comités interinstitucionales, plataformas de múltiples interesados) que incluyan las asociaciones público-privadas con propietarios, operadores o administradores de infraestructura crítica.

Personas y Habilidades

Hay varias habilidades que los Estados miembros deben tener en cuenta al implementar esta norma. Por un lado, **habilidades técnicas** para mejorar la ciberseguridad de la infraestructura crítica y la respuesta y gestión de incidentes de TIC (p. ej., seguridad de las redes, análisis forense digital, etc.). Por otro, los Estados miembros deben realizar **entrenamientos y ejercicios que pongan a prueba la continuidad del servicio y los planes de contingencia** ante incidentes que afecten la infraestructura crítica y deben alentar a las partes interesadas a que participen en actividades similares. Por último, el personal diplomático debe tener las habilidades necesarias para **interactuar con sus homólogos en el tema específico de la infraestructura crítica**, en particular si la infraestructura es transnacional.

Tecnología

En términos de tecnología, se recomienda que los Estados miembros tengan la **capacidad técnica para prevenir, detectar e interrumpir actos maliciosos con TIC dirigidos a las infraestructuras críticas**. Estos pueden incluir, entre otros, plataformas de inteligencia sobre amenazas,[32] sistemas de alerta temprana,[33] herramientas para el escaneo de vulnerabilidades[34] y perímetros seguros.[35]

---

32 Una plataforma de inteligencia sobre amenazas automatiza la recopilación, agregación y conciliación de datos de amenazas externas; véase https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/threat-intelligence-platforms/#:~:text=A%20threat%20intelligence%20platform%20automates,risks%20relevant%20for%20their%20organization).

33 Un sistema de alerta temprana es un servicio de notificación de amenazas que reporta actividades potencialmente sospechosas en la red; véase https://www.ncsc.gov.uk/blog-post/early-warning-whats-new-and-whats-in-it-for-you.

34 Son herramientas automatizadas para descubrir, analizar e informar sobre fallas de seguridad y vulnerabilidades en una red.

35 Por ejemplo, mediante la implementación de soluciones con aislamiento físico (air-gapped: sin conexión entre redes locales y externas) o con el uso de firewalls.

3.8 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. Los Estados también deben responder a las solicitudes apropiadas para mitigar las actividades maliciosas con TIC dirigidas a la infraestructura crítica de otro Estado y originadas en su territorio, con el debido respeto a su soberanía.

Políticas y Reglamentos

El texto de esta norma contiene varios conceptos y responsabilidades que los Estados miembros deben aclarar. Por lo tanto, una **interpretación nacional de esta norma** ayudaría a los Estados miembros a precisar lo que quieren decir con, por ejemplo, "solicitudes apropiadas" o "infraestructura crítica" (véase también la Norma G). Es importante que los Estados miembros promulguen posteriormente legislación que proporcione un **marco para la solicitud y la prestación de asistencia internacional** y **estrategias y políticas de ciberseguridad** que detallen los mecanismos, procedimientos y procesos para iniciar, enviar y responder a solicitudes de asistencia.

Estructuras y Procesos

Dada la perspectiva transnacional y cooperativa de la norma, los Estados miembros deberían establecer **mecanismos eficientes para recibir, procesar, evaluar y responder solicitudes de asistencia, así como para prepararlas y enviarlas**.[36] Además, teniendo en cuenta la dimensión coercitiva de la norma, que insta a los Estados miembros a mitigar las actividades de TIC maliciosas originadas en su territorio, se recomienda que los Estados miembros establezcan **las capacidades necesarias para la aplicación del derecho cibernético.**

Asociaciones y Redes

A escala internacional, los Estados miembros deben unirse a **instrumentos o acuerdos bilaterales, regionales y multilaterales de cooperación para la protección de infraestructura crítica**. Estas redes pueden ayudar a gestionar las solicitudes de asistencia (por ejemplo, pueden tener plantillas comunes disponibles o mecanismos específicos para la comunicación en casos de crisis o la gestión de incidentes que los Estados miembros pueden activar). Además, dado el papel que desempeñan los actores no estatales (a menudo internacionales) en la gestión de la infraestructura crítica, es importante establecer una

36 Los mecanismos eficientes para recibir y enviar solicitudes de información pueden incluir la creación de plantillas o documentos orientadores sobre qué información se incluirá en las solicitudes, el establecimiento de puntos de contacto para asuntos técnicos y un comité ad hoc u otra entidad para evaluar la idoneidad de un pedido.

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). A escala nacional se recomienda promover la cooperación entre las partes interesadas pertinentes para la protección de infraestructura crítica (p. ej. asociaciones público-privadas y comités interinstitucionales. Estas disposiciones ayudarían a aumentar el intercambio de información y llevar a cabo intervenciones oportunas y eficientes.

Personas y Habilidades

Para implementar esta norma los Estados miembros deberían tener **personal capacitado para gestionar la asistencia transfronteriza en la protección de infraestructuras críticas** (p. ej., investigadores de ciberseguridad, especialistas en gestión de riesgos en las cadenas de suministro y personal de respuesta a incidentes). Por otra parte, una solicitud de asistencia puede referirse a diversos aspectos de la protección de infraestructura crítica; por lo tanto, el personal que recibe o envía las solicitudes de asistencia debe entender claramente **cómo atender y gestionar una solicitud de asistencia.**

Tecnología

En términos de tecnología, es importante que los Estados miembros desarrollen las **capacidades necesarias para prevenir, detectar e interrumpir actos maliciosos con TIC dirigidos a las infraestructuras críticas.** Estos pueden incluir, entre otros, plataformas de inteligencia sobre amenazas,[37] sistemas de alerta temprana[38] y herramientas para el escaneo de vulnerabilidades.[39] Adicionalmente, dado que la norma se centra en la asistencia, los Estados miembros deben establecer **canales de comunicación o plataformas seguras** para el intercambio de información relacionada con actos maliciosos contra infraestructuras críticas.

37 Una plataforma de inteligencia sobre amenazas automatiza la recopilación, agregación y conciliación de datos de amenazas externas; véase https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/threat-intelligence-platforms/#:~:text=A%20threat%20intelligence%20platform%20automates,risks%20relevant%20for%20their%20organization).

38 Un sistema de alerta temprana es un servicio de notificación de amenazas que reporta actividades potencialmente sospechosas en la red; véase https://www.ncsc.gov.uk/blog-post/early-warning-whats-new-and-whats-in-it-for-you.

39 Son herramientas automatizadas para descubrir, analizar e informar sobre fallas de seguridad y vulnerabilidades en una red.

3.9 Norma I

Los Estados deben 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 prevenir la proliferación de herramientas y técnicas de TIC maliciosas y el uso de funciones dañinas ocultas.

Políticas y Reglamentos

Teniendo en cuenta la complejidad y la estructura en varios niveles de las cadenas de suministro contemporáneas, es importante que los Estados miembros definan **su interpretación nacional de la norma** (p. ej., especificando lo que entienden por "medidas razonables"). También se recomienda que los Estados miembros promulguen **legislación que prohíba la introducción de funciones ocultas dañinas y la explotación de vulnerabilidades en productos de TIC.**[40] Esto proporcionaría la base jurídica para prevenir (y procesar judicialmente) actos maliciosos contra la cadena de suministro. Además, es importante que los Estados miembros adopten **una política o estrategia de ciberseguridad que abarque la seguridad de la cadena de suministro**, quizá mediante la descripción general de un marco para la gestión de riesgos en la cadena de suministro basado en una evaluación de riesgos que tenga en cuenta una variedad de factores, incluidos los beneficios y riesgos de las nuevas tecnologías. Por último, para evitar el surgimiento de múltiples y diferentes marcos para la regulación de la seguridad de la cadena de suministro, se recomienda que los Estados miembros establezcan los **requisitos para implementar reglas y estándares comunes interoperables a nivel mundial para la seguridad de la cadena de suministro** (p. ej., ISO/IEC 20243). Teniendo en cuenta todos los aspectos de seguridad implicados en la producción de productos de TIC, los Estados miembros deben solicitar a los proveedores **que incorporen la seguridad y la protección en la gestión del ciclo de vida de sus productos.**

Estructuras y Procesos

Para implementar esta norma los Estados miembros deben implementar **mecanismos 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. Esto es especialmente importante porque les permitiría a los Estados miembros identificar, monitorear y evaluar los

40 Algunos ejemplos adicionales de posibles intervenciones legislativas son: medidas para evitar la manipulación de productos y servicios durante el desarrollo y la producción, si hacerlo podría perjudicar sustancialmente la estabilidad del ciberespacio, y medidas para prohibir que cualquier persona dentro de su territorio o jurisdicción participe en operaciones cibernéticas que puedan poner en peligro la seguridad, integridad o confidencialidad de los productos y servicios comerciales de TIC.

riesgos en la cadena de suministro.[41] Por otra parte, en términos de estructura, se recomienda que los Estados miembros introduzcan **un mecanismo de evaluación y certificación,** ya sea mediante la creación de una entidad nacional dedicada o la asociación con otros Estados que ya tengan esta capacidad. Por último, los Estados miembros deberían **garantizar la interoperabilidad** (entre jurisdicciones) de enfoques, métodos de certificación y certificaciones de productos de TIC.

Asociaciones y Redes

Dadas las dimensiones transnacionales de la mayoría de las cadenas de suministro, los Estados miembros deberían desarrollar **medidas de cooperación bilaterales, regionales y multilaterales** para, por ejemplo, intercambiar buenas prácticas de gestión de riesgos en la cadena de suministro o la certificación de productos de TIC, e intercambiar información sobre vulnerabilidades relacionadas con las TIC o funciones ocultas dañinas en los productos.

Personas y Habilidades

Hay varios conjuntos de habilidades que los Estados miembros deben tener en cuenta al implementar esta norma. Primero, **habilidades técnicas y organizativas** para gestionar la seguridad de las cadenas de suministro. Estas incluyen, entre otras, habilidades para identificar, monitorear e intervenir para resolver las vulnerabilidades de la cadena de suministro y evaluar su resiliencia. Luego, **ante** actos maliciosos con TIC también son fundamentales las **habilidades de respuesta a incidentes y su gestión.** Por último, dada la importancia de las cadenas de suministro para la seguridad internacional, es relevante que el **personal diplomático** de los Estados Miembros **sea capaz de interactuar significativamente** con sus homólogos en relación con **el tema específico de la seguridad de las cadenas de suministro.**

Tecnología

Es importante que los Estados miembros cuenten con la **capacidad técnica para prevenir, detectar o interrumpir ataques a las cadenas de suministro.** Estas capacidades pueden incluir, entre otras, plataformas de inteligencia sobre amenazas[42] y sistemas de alerta temprana.[43] Los Estados miembros (en caso de que deseen evaluar productos de TIC) también deberían tener herramientas disponibles para la obtención de códigos-fuente (*code sourcing*) y el *fuzzing* de código.[44]

---

41 Con este fin, los Estados miembros pueden obligar a los proveedores a utilizar la denominada Lista de materiales de software (SBOM, por sus siglas en inglés, que son inventarios que enumeran todos los componentes del software), ya que esto permitiría a los Estados miembros evaluar rápidamente si, en primer lugar, existe un riesgo para la cadena de suministro.

42 Una plataforma de inteligencia sobre amenazas automatiza la recopilación, agregación y conciliación de datos de amenazas externas; véase **https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/threat-intelligence-platforms/#:~:text=A%20threat%20intelligence%20platform%20automates,risks%20relevant%20for%20their%20organization)**.

43 Un sistema de alerta temprana es un servicio de notificación de amenazas que reporta actividades potencialmente sospechosas en la red; véase **https://www.ncsc.gov.uk/blog-post/early-warning-whats-new-and-whats-in-it-for-you**.

44 *Code sourcing* y *code fuzzing* son dos métodos para encontrar y enfrentar vulnerabilidades en el código del software.

3.10 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

Para implementar adecuadamente la norma es muy importante que los Estados Miembros elaboren su **interpretación nacional de la norma**, y que esta abarque, por ejemplo, cómo interpretan "notificación responsable" y "compartir la información [...] soluciones disponibles". Desde una perspectiva legislativa, es clave que posteriormente los Estados miembros adopten **medidas legales para frenar la distribución comercial de vulnerabilidades** (por ejemplo, estableciendo límites estrictos al desarrollo, almacenamiento y venta de vulnerabilidades de TIC por parte de actores del sector privado con el fin de obtener ganancias financieras) y para **despenalizar y proteger a los investigadores de ciberseguridad y los** *hackers* **éticos** que desean identificar vulnerabilidades. Es igualmente e importante **establecer una política de divulgación coordinada de vulnerabilidades (CVD)** (puede incluirse en la estrategia o política de seguridad cibernética o adoptarse como instrumento independiente) basada en la suposición de la divulgación privada por encima de la contención de vulnerabilidades.[45] Con el fin de compartir información sobre nuevas vulnerabilidades y soluciones disponibles también se recomienda implementar **marcos legales que permitan la cooperación y el intercambio de información con vendedores y proveedores**. En cuanto a los vendedores y proveedores, es pertinente que los Estados miembros establezcan con precisión los **requisitos necesarios para que las políticas y prácticas de gestión de vulnerabilidades sean eficientes y eficaces** en minimizar los posibles efectos adversos de los productos vulnerables y sistematizar la comunicación de vulnerabilidades de TIC.

Estructuras y Procesos

Los Estados miembros deben establecer los procesos y estructuras necesarios para que la política de divulgación coordinada de vulnerabilidades funcione correctamente.[46] Como indica el informe de 2021 del GEG, esto debería incluir una **orientación sobre**

45 Entendemos que algunos Estados, en ciertas circunstancias, podrían preferir no revelar las vulnerabilidades. En estos casos recomendamos desarrollar una política de acciones ante vulnerabilidades (vulnerability equities policy) que permita a los Estados miembros evaluar caso por caso si deben difundir la información de vulnerabilidad o restringirla temporalmente con fines de seguridad nacional o aplicación de la ley.

46 Hay buenos recursos de dominio público para apoyar a los Estados en el diseño de su aparato nacional de CVD; véase por ejemplo **https://elearning.osce.org/courses/course-v1:OSCE+TNTD-CYBERCVD+2022_04/about**.

las respectivas funciones y responsabilidades de las diferentes partes interesadas en los procesos de divulgación, los tipos de información técnica que se divulgará o compartirá públicamente, y el manejo de datos confidenciales para garantizar la seguridad y la confidencialidad de la información. Además, los Estados miembros deben crear **protocolos para la comunicación e intercambio de información entre todos los interesados pertinentes** (p. ej., gobiernos, proveedores y vendedores, investigadores de seguridad y equipos de respuesta a incidentes) y para **compartir actualizaciones y parchear sistemas**. Es importante que posteriormente implementen incentivos (p. ej., programas de recompensa por detección de fallos) y, como indica el informe de 2021 del GEG, orientación sobre la divulgación coordinada de vulnerabilidades (p. ej., claridad sobre las respectivas funciones y responsabilidades de las diferentes partes interesadas en los procesos de divulgación, los tipos de información técnica que se divulgará o compartirá públicamente y el manejo de datos confidenciales).[47] Por último, sería fundamental implementar **campañas sistemáticas de concienciación** (dirigidas tanto al público en general como al personal de sectores específicos) sobre la importancia de los parches de seguridad.

Asociaciones y Redes

Teniendo en cuenta las dimensiones intersectoriales y transnacionales de la divulgación responsable de vulnerabilidades, conviene desarrollar una **cooperación bilateral, regional y multilateral** en esta materia. De hecho, el informe de 2021 del GEG menciona la cooperación internacional como un elemento fundamental de "un proceso confiable y consistente para hacer rutinarias las divulgaciones".[48] **Establecer una cooperación intersectorial** con el sector privado, la sociedad civil y la comunidad técnica, incluidos vendedores y propietarios, es igual de importante.

Personas y Habilidades

Hay tres conjuntos diferentes de habilidades que son importantes para la implementación de esta norma. En primer lugar, las **habilidades técnicas**, entre ellas capacidades para identificar y resolver vulnerabilidades o gestionar la información relacionada con vulnerabilidades (p. ej., información proporcionada por empresas que ofrecen recompensa por detección de fallos, investigadores de seguridad y proveedores). En segundo lugar, las **habilidades de comunicación pública** también son relevantes, especialmente cuando es vital dirigirse al público en general respecto de vulnerabilidades que tengan impacto en la población. Finalmente, en vista del posible impacto de las vulnerabilidades en la seguridad internacional, se necesitan **habilidades diplomáticas y de comunicación** para poder participar exitosamente en las discusiones sobre gestión de vulnerabilidades con los Estados y los actores no estatales pertinentes.

---

47 Los gobiernos que deseen conservar la posibilidad de contención y no divulgación deben desarrollar un proceso específico, descrito en un documento público, para gestionar cuándo y cómo un gobierno elegirá divulgar las vulnerabilidades cibernéticas que descubra o compre. Este proceso debe incluir, por ejemplo, un comité interinstitucional para la evaluación de vulnerabilidades, criterios claros para determinar si se debe divulgar una vulnerabilidad, y el mecanismo de gestión de desacuerdos dentro del comité. Véase, por ejemplo: **https://trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF.**

48 **GGE. 2021**, para. 61.

Tecnología

Existen **capacidades técnicas específicas para identificar y resolver vulnerabilidades de TIC** que resultan pertinentes para implementación de la norma. Estas incluyen, entre otras, herramientas para el escaneo y la evaluación de vulnerabilidades, para el intercambio de explotabilidad de vulnerabilidades (VEX)[49] y para **aplicar parches a gran escala**, como software de gestión de parches.

49 "El intercambio de explotabilidad de vulnerabilidades (VEX) es un sistema que usan los productores de software para compartir con los consumidores de software una evaluación de las vulnerabilidades presentes en sus componentes de software. VEX es el mecanismo mediante el cual los productores de software clasifican y etiquetan las vulnerabilidades de su software. [...] También incluyen un análisis de las vulnerabilidades; por ejemplo, si la vulnerabilidad puede o no ser explotable y por qué, y cómo puede mitigarse o corregirse la vulnerabilidad, así cualquier solución alternativa conocida que pueda usarse para protegerse contra ella"; véase https://www.endorlabs.com/blog/what-is-vex-and-why-should-i-care.

3.11 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

Con el fin de aplicar correctamente la norma los Estados miembros deben esbozar su **posición sobre la norma** o sobre ciertos aspectos de ella. Por ejemplo, es fundamental definir la posición nacional sobre la aplicabilidad del derecho internacional en materia del uso de las TIC por parte de los Estados y sobre los conceptos de "actividades internacionales maliciosas" y "apoyar a sabiendas". Se recomienda que un Estado miembro, para indicar ante la comunidad internacional su compromiso de respetar la norma, publique una **declaración en la que manifieste que no utilizará equipos autorizados de respuesta a emergencias para participar en actividades internacionales maliciosas u ofensivas.** Como señal para otros Estados es igualmente importante que los Estados miembros declaren en **una lista cuáles son todos los CSIRT/CERT en su territorio.** En el ámbito nacional, los Estados miembros deben describir claramente en su política o estrategia de ciberseguridad el **estado, la autoridad y los mandatos de sus CERT/CSIRT**, junto lo que distingue sus funciones únicas y neutrales de otras funciones gubernamentales. Por último, dada la función neutral y única de estos equipos de detección y respuesta a incidentes cibernéticos, es importante establecer un **marco regulatorio para el trabajo de los CERT/CSIRT que esté alineado con las pautas y normas internacionales** (p. ej., el código ético de FIRST o ISO 27/2001).

Estructuras y Procesos

Si bien la norma no exige que los Estados Miembros establezcan capacidades nacionales (o regionales) de respuesta a incidentes cibernéticos, como las capacidades indicadas en la Norma A, se recomienda que los Estados Miembros **establezcan un CSIRT/CERT nacional o que se unan a uno regional.** Por otra parte, considerando el propósito de la norma, es importante que los Estados miembros establezcan **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 (p. ej., un comité parlamentario).

Asociaciones y Redes

Este estudio no identificó ninguna capacidad fundamental, en términos de asociaciones y redes, necesaria para implementar esta norma.

Personas y Habilidades

Es muy importante que los Estados miembros puedan identificar y documentar posibles casos de uso indebido de los CSIRT/CERT en actividades maliciosas. Por lo tanto, los Estados miembros deben disponer de **expertos que lleven a cabo la investigación técnica de estas actividades** (p. ej., analistas forenses de TIC) o, en caso de que la investigación técnica sea realizada por un tercero, que puedan evaluar su calidad. Además, es importante que **los funcionarios públicos** (incluidas las fuerzas armadas) **estén conscientes** de la función y la condición de los CERT/CSIRT. Finalmente, los **conocimientos jurídicos especializados, entre otras áreas en el derecho internacional específico para el ámbito de las TIC**, es clave para implementar adecuadamente varios elementos (p. ej., redactar la interpretación nacional de la norma) relacionados con la implementación de la norma.

Tecnología

Este estudio no identificó ninguna capacidad tecnológica fundamental necesaria para implementar esta norma.

4. Derecho Internacional

El capítulo anterior señaló elementos específicos del derecho internacional pertinentes en normas específicas. Esta sección brinda una descripción más general de las FCC relacionadas con el derecho internacional que trascienden los requisitos específicos de las normas descritas anteriormente. El informe sustantivo del GTCA de 2019-2021 subraya que, "[r]econociendo la Resolución de la Asamblea General 70/237 y la resolución de la Asamblea General 73/27, que estableció el GTCA, los Estados reafirmaron que el derecho internacional, y en particular la Carta de las Naciones Unidas, es aplicable y esencial para mantener la paz y la estabilidad y promover TIC abiertas, seguras, estables, accesibles y pacíficas".[50]

Políticas y Reglamentos

Los Estados miembros acordaron que el derecho internacional es aplicable a las TIC y que "es necesario desarrollar más entendimientos comunes sobre cómo aplicar el derecho internacional al uso estatal de las TIC".[51] Para promover el desarrollo de un entendimiento común sobre cómo aplicar el derecho internacional, se recomienda que los Estados miembros elaboren e intercambien

50 **OEWG. 2021. Final Substantive Report**, párr. 34.
51 Ibid.

sus correspondientes puntos de vista. Como punto de partida, los Estados deberían desarrollar **posiciones nacionales públicas sobre la aplicabilidad del derecho internacional en el contexto de las TIC.**

Estructuras y Procesos

Se recomienda que, para garantizar que el comportamiento de los Estados miembros en el ciberespacio y su uso de TIC sea legal, y para hacerlos responsables por sus actos, los Estados miembros establezcan (a escala nacional o regional) un **mecanismo de supervisión independiente** (judicial, administrativo, parlamentario).

Asociaciones y Redes

En vista de los desafíos actuales concernientes al desarrollo de un entendimiento común sobre cómo aplicar el derecho internacional al uso de las TIC, es importante que los Estados miembros proponga **mecanismos de cooperación** (p. ej., compartir lecciones aprendidas, establecer programas de visitas para expertos legales, intercambiar información) en las áreas de derecho internacional y legislaciones y políticas nacionales. También se recomienda que los Estados miembros **participen activamente en los procesos multilaterales relacionados con el derecho internacional en el ámbito de las TIC** (p. ej., el GTCA).

Personas y Habilidades

Aplicar el derecho internacional en el ámbito de las TIC o desarrollar una visión nacional sobre el tema requiere que los Estados desarrollen u obtengan **acceso a conocimientos jurídicos especializados.** También es fundamental que los Estados miembros puedan participar en **discusiones regionales e internacionales sobre derecho internacional**, lo cual incluye interactuar con la comunidad académica y la sociedad civil en general. Se recomienda que, en estos contextos, los expertos y profesionales jurídicos puedan participar de manera significativa en actividades realizadas en un idioma diferente de su lengua materna.

Tecnología

Este estudio no identificó ninguna capacidad tecnológica fundamental necesaria para implementar esta norma.

5. Medidas de Fomento de la Confianza

Al igual que con el derecho internacional, en las diversas secciones del capítulo 3 se mencionaron las medidas de fomento de la confianza específicas para las normas. Este capítulo aporta una descripción más general de medidas adicionales para el fomento de la confianza que los Estados deberían considerar implementar a escala nacional. Como afirmó el informe sustantivo del primer GTCA, "[l]as medidas de fomento de la confianza (MFC), que comprenden medidas de transparencia, cooperación y estabilidad, pueden contribuir a prevenir conflictos, evitar percepciones erróneas y malentendidos, y reducir tensiones. Son una expresión concreta de la cooperación internacional".[52] El informe describe las FCC relacionadas con las MFC.

Políticas y Reglamentos

En términos de políticas y normas para el fomento de la transparencia, se recomienda que los Estados Miembros **divulguen públicamente todas las estrategias, políticas y reglamentos nacionales relevantes de seguridad cibernética**, idealmente con una

52 **OEWG. 2021. Final Substantive Report**, párr. 34.

traducción oficial al inglés (como mínimo) para facilitar el acceso a ellas. Por otra parte, es importante que los Estados miembros **identifiquen y consideren las MFC adecuadas a su contexto específico** y adopten políticas y reglamentos para cooperar en su implementación con otros Estados (p. ej., adoptar plantillas para compartir información o establecer puntos de contacto a nivel nacional).

Estructuras y Procesos

El **establecimiento de un punto de contacto** es uno de los elementos esenciales para fomentar la confianza. Establecer puntos de contacto a nivel técnico y diplomático es importante para garantizar la comunicación directa entre los Estados miembros, aspecto clave no solo en relación con la implementación de normas específicas, sino especialmente en tiempos de crisis. Además, para fomentar la transparencia, la cooperación y la estabilidad, los Estados miembros deben desarrollar **capacidades de respuesta a incidentes cibernéticos nacionales o regionales (p. ej., un CERT/CSIRT).** Debido a su función de "primera respuesta", estas estructuras desempeñan una función fundamental para enfrentar incidentes o amenazas tan pronto como se produzcan. Y frecuentemente esto implica interactuar con sus homólogos en el extranjero. A su vez, estas interacciones contribuyen a aumentar la transparencia y la cooperación. En cuanto a los procesos, es muy importante que los Estados miembros **compartan información y buenas prácticas sobre varios temas relacionados,** incluidos las amenazas e incidentes de TIC existentes y emergentes, los estándares de análisis de vulnerabilidad de los productos de TIC, así como el intercambio de información sobre los enfoques nacionales de la seguridad de las TIC y la protección de datos. Para este fin los Estados Miembros pueden utilizar el Portal de Política Cibernética del Instituto de las Naciones Unidas de Investigación sobre el Desarme.[53]

Asociaciones y Redes

Es posible implementar medidas de fomento de la confianza siempre que los Estados miembros participen con otros en entornos internacionales. Por lo tanto, se recomienda que los Estados miembros **participen en los procesos de las Naciones Unidas** (como el GTCA, que ha sido reconocido en sí mismo como una medida de fomento de la confianza), en **diálogos a través de consultas bilaterales, subregionales, regionales y multilaterales**, y que interactúen con los **organismos regionales que desarrollaron e implementaron MFC.** Además, es muy importante que los Estados miembros **participen en marcos de cooperación entre CERT/CSIRT** u otros organismos técnicos de seguridad, como la red FIRST u otros marcos regionales. Estos marcos ofrecen una oportunidad única para desarrollar relaciones que aumentan la confianza entre la comunidad técnica.

Personas y Habilidades

Los Estados miembros deben retener expertos con **conocimiento de las MFC** y las maneras de activarlas o aprovecharlas en momentos de crisis. En particular, dado el papel clave de los PoC, se recomienda tener **personal preparado para actuar eficazmente como PoC** (p. ej., impartir capacitación sobre la función y los procesos de PoC). También es importante que los Estados miembros dispongan de personal capaz de **hacer uso de**

53 https://cyberpolicyportal.org/.

plataformas de intercambio de información (p. ej., el portal de políticas cibernéticas de UNIDIR), que se consideran herramientas importantes para el fomento de la transparencia. Por último, el fomento de la confianza requiere funcionarios públicos con **habilidades comunicativas y diplomáticas** que puedan participar con sus homólogos en debates sobre ciberseguridad.

Tecnología

Los **canales y las plataformas confiables de comunicación** entre los Estados son importantes para fomentar la confianza en las relaciones.

6. Conclusiones

Dado que el panorama de las ciberamenazas evoluciona continuamente, es importante que los Estados maximicen su capacidad para prevenir o mitigar las consecuencias de actos maliciosos que impliquen TIC. Como parte de este esfuerzo, poder implementar el Marco de Comportamiento Responsable de los Estados en el ciberespacio es un paso importante para aumentar la resiliencia cibernética nacional y también un paso necesario para garantizar la paz y la seguridad en el ámbito de las TIC.

El propósito de las capacidades cibernéticas fundamentales identificadas en este informe es que representen las condiciones iniciales a partir de las cuales se pueden desarrollar medidas más elaboradas o avanzadas. No obstante, la lista de capacidades identificadas no debe considerarse cerrada ni definitiva. Dados los continuos y rápidos desarrollos en el ámbito de las TIC (p. ej., la adopción generalizada de nuevas tecnologías disruptivas como la inteligencia artificial o la computación cuántica), elementos adicionales podrían llegar a ser relevantes y fundamentales para las normas existentes o para el desarrollo de nuevas normas.

Cabe señalar que, si bien el propósito de este estudio no es clasificar o asignar "pesos" específicos a las FCC o a normas individuales, un análisis de la distribución general de FCC sugiere que cinco elementos clave emergen como particularmente prominentes:

a. una estrategia o política nacional integral de seguridad cibernética;
b. una entidad dedicada a actuar como entidad de enlace o coordinadora nacional en asuntos cibernéticos;
c. la capacidad de respuesta a emergencias o incidentes (nacional o regional);
d. una cooperación bien estructurada entre todas las partes interesadas pertinentes, incluido el sector privado y los operadores de infraestructuras críticas; y
e. el acceso a habilidades especializadas (p. ej., técnicas, legales, diplomáticas, comunicacionales).

Estos cinco elementos clave se encuentran entre las capacidades más recurrentes que resultan relevantes en casi todos los componentes del Marco. Por lo tanto, mediante el desarrollo de estos elementos los Estados miembros pueden beneficiarse de la implementación de todo el Marco. Además, como se mencionó en el capítulo 2, es muy importante que los Estados miembros, al implementar las capacidades cibernéticas fundamentales, lo hagan respetando plenamente los derechos humanos y teniendo en cuenta las dimensiones de género. Futuros esfuerzos de investigación podrían desglosar aún más cada pilar o elemento de las FCC con el fin de profundizar en la comprensión de las dinámicas de género presentes y enmarcar mejor su formulación e implementación.

Las FCC que presenta este informe constituyen los elementos a través de los cuales los Estados miembros pueden implementar el Marco y fomentar la paz, la seguridad, la cooperación y la confianza internacionales en el entorno de las TIC. La segunda parte de este estudio, titulada "Introducción a un enfoque basado en amenazas", propone un enfoque que permitiría a los gobiernos evaluar mejor su preparación para aprovechar el Marco y prevenir o responder a actividades y amenazas maliciosas específicamente relacionadas con TIC.

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

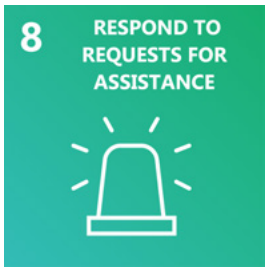
Un Estado no debe realizar ni apoyar a sabiendas una actividad con TIC contraria a sus obligaciones en virtud del derecho internacional que dañe o perjudique intencionalmente la infraestructura crítica.

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