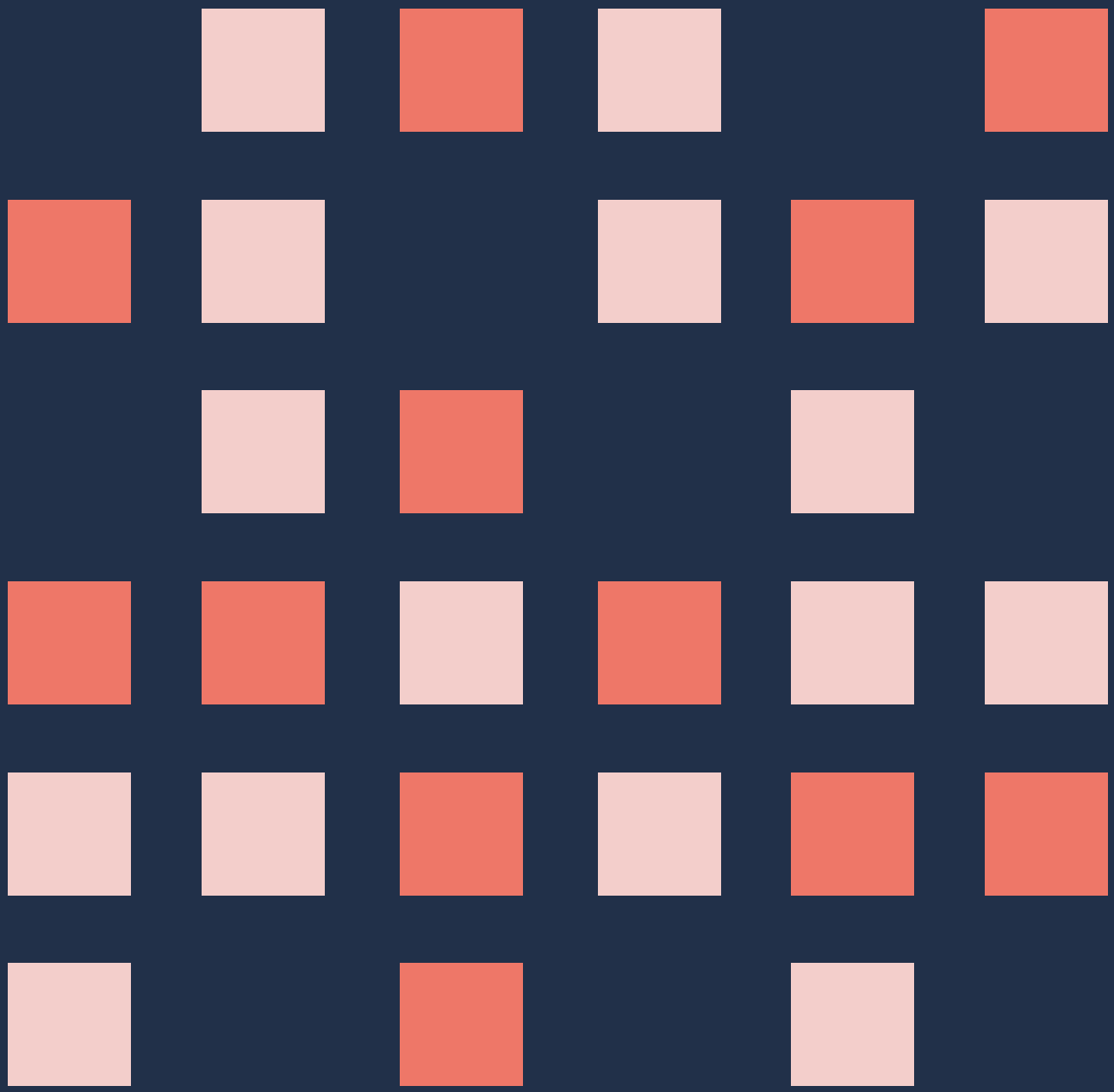
Guía para Cibernormas Inclusivas



GLOBAL PARTNERS DIGITAL

2023

Agradecimientos

Esta publicación fue elaborada por Global Partners Digital. Su desarrollo no hubiera sido posible sin la participación de las siguientes expertas, quienes con sus aportes y conocimientos contribuyeron a su desarrollo y redacción:

- Verónica Ferrari, Asociación para el Progreso de las Comunicaciones (APC)
- Dra. Katharine M Millar, Departamento de Relaciones Internacionales, London School of Economics
- Allison Pytlak, Stimson Center (previamente WILPF)
- Dra. Tatiana Tropina, Institute of Security and Global Affairs, Leiden University.

Agradecemos, además, a las siguientes personas, que fueron parte de consultas llevadas a cabo por Verónica Ferrari durante el desarrollo de la guía:

- Adeboye Adegoke, Paradigm Initiative
- Vivian Affoah, Media Foundation for West Africa
- Enrico Calandro, Cyber Resilience for Development (Cyber4Dev)
- Lillian Nalwoga, Collaboration on International ICT Policy in East and Southern Africa (CIPESA).

Finalmente, agradecemos a Isabel Lecaros por su trabajo de diseño y diagramación de esta publicación, y a Ana Pleite por su traducción al español.

El desarrollo de esta publicación fue posible gracias al apoyo financiero de Global Affairs Canada.

Índice

Preámbulo

Por qué se creó este conjunto de herramientas

El objetivo de las cibernormas es crear un ciberespacio pacífico y seguro mediante la delimitación de las conductas de los y las agentes en ese entorno y la definición de la respuesta a las amenazas.

No obstante, no todas las personas viven el ciberespacio de la misma manera. Las partes interesadas marginadas —incluidas las mujeres, las comunidades LGBT+, los grupos racializados, las personas del Sur Global y quienes ejercen profesiones vulnerables (por ejemplo, activistas y personas que realizan investigación en materia de seguridad)— se enfrentan a riesgos específicos y de mayor alcance en el entorno digital: desde el acoso y el hostigamiento hasta la piratería informática patrocinada por el Estado. Es posible que también se enfrenten a obstáculos específicos para ejercer sus derechos humanos en el ciberespacio, desde limitaciones económicas y barreras lingüísticas a brechas en el acceso.

Pese a ello, en los procesos establecidos con el fin de formular normas que regulen el ciberespacio apenas se presta atención a la inclusión de estos grupos marginados. No están suficientemente representados y no se les consulta. Incluso cuando técnicamente sí se toman en consideración factores como el género, la raza y la sexualidad, a menudo se hace de forma superficial o sin matices. En consecuencia, la aplicación de las cibernormas no solo no responde adecuadamente a las circunstancias de las comunidades marginadas, sino que puede incluso empeorarlas.

¿Cuál es la solución? Un enfoque rigurosamente integrador para la elaboración e implementación de cibernormas. Eso es precisamente lo que se pretende promover y facilitar con este conjunto de herramientas.

A partir de una amplia labor de investigación y consulta con diversas partes interesadas y con personas expertas vinculadas a los procesos en curso en materia de cibernormas —incluido el Grupo de Trabajo de Composición Abierta (GTCA) de las Naciones Unidas sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional—, en estas herramientas se ofrecen orientaciones concretas y adaptadas para integrar la inclusión en la elaboración y aplicación de normas mediante los procesos de formulación de políticas, incluidas:

- → Una introducción a los términos y conceptos clave relacionados con la inclusión y las cibernormas;
- → Una guía práctica en cinco pasos para crear un proceso inclusivo de elaboración de cibernormas o de implementación de las normas ya acordadas;
- → Un conjunto complementario de recursos prácticos para facilitar la implantación de procesos inclusivos de elaboración de políticas;

Herramienta 1	Mapeo de las partes interesadas de forma inclusiva.
Herramienta 2	Explicación básica para entender la terminología de la inclusión.
Herramienta 3	Explicación básica con un mapeo de procesos regionales e internacionales de elaboración de cibernormas.

En esta sección se exponen los fundamentos de las cibernormas y los argumentos a favor de un enfoque integrador.

Sección 1

¿Por qué la elaboración e implementación de cibernormas deben realizarse a través de procesos inclusivos?

¿Qué es una cibernorma?

Por «norma» se entiende una interpretación común de las conductas consideradas adecuadas para los y las agentes de un ámbito determinado.

Por tanto, las cibernormas, en grandes líneas, se refieren al comportamiento que se espera de los y las agentes (Estados, empresas privadas, organizaciones de la sociedad civil, particulares, etc.) en el ciberespacio, en relación con el uso de las tecnologías digitales.

Pueden adoptar diversas formas. Pueden ser principios comunes (como el consenso general sobre la necesidad de respetar los derechos humanos en Internet) y pueden presentarse como compromisos escritos, voluntarios y no vinculantes, acuerdos, marcos normativos o declaraciones de principios. Algunos ejemplos son las **once normas del Grupo de Expertos Gubernamentales (GEG) de las Naciones Unidas**, el **Marco de Gestión de Datos de la ASEAN** y el **Manual de Tallin**.

Uno de los principales objetivos de las cibernormas es limitar y atajar las ciberamenazas, que también pueden adoptar diversas formas: desde grandes ciberataques patrocinados por el Estado hasta piratería informática, acoso y hostigamiento. Las cibernormas pueden, asimismo, tener una dimensión positiva, al establecer mecanismos de capacitación, protección y promoción de la cooperación y de las políticas basadas en el respeto de los derechos. Para que surtan el efecto deseado, estos compromisos suelen traducirse y aplicarse mediante la elaboración de políticas y marcos normativos nacionales o regionales, como, por ejemplo, estrategias de ciberseguridad generales, políticas de ciberseguridad específicas para cada tema, y reglamentación.

¿En qué consiste un enfoque que incluya a las comunidades marginadas?

Los enfoques inclusivos en las labores normativas se basan en la idea de que la inclusión de las partes interesadas en el proceso tiene un valor tanto intrínseco como práctico, como exponemos en nuestra guía para la elaboración inclusiva de estrategias nacionales de ciberseguridad. Es decir, no solo es el planteamiento correcto desde el punto de vista ético, dado que recoge tanto los derechos humanos como los principios democráticos, sino que además se traduce en políticas y normativas más eficaces y de mayor impacto.

En términos generales, un enfoque integrador de la elaboración de cibernormas debe aspirar a una inclusión significativa de:

1. las personas con un mandato, función o responsabilidad en el proceso;
2. las personas con las competencias o conocimientos necesarios para elaborar la normativa y ponerla en práctica;
3. las personas que podrían verse desproporcionadamente afectadas por la normativa o su aplicación, es decir, los grupos marginados.

Este conjunto de herramientas se centra particularmente en el tercer punto (aunque, por supuesto, todos ellos se solapan), con el objetivo de exponer las consideraciones, las sensibilidades y los ajustes específicos que deben tenerse en cuenta para garantizar que los grupos marginados puedan participar realmente en esos procesos.

Los recursos que se ofrecen a continuación —incluida una guía paso a paso para incluir a los grupos marginados en todas las fases del proceso normativo, además de herramientas para tareas y componentes específicos— constituyen una orientación a la vez concreta y detallada. Al mismo tiempo, se basan en principios generales que todo proceso verdaderamente integrador debe incorporar: la apertura y la aceptación de distintos tipos de aportes; el fomento del consenso mediante la comprensión y la confianza mutuas; y una comunicación clara y transparente sobre el proceso y sus resultados.

En esta sección, se propone un proceso de cinco etapas para garantizar que esos procesos y sus resultados se lleven a cabo de forma inclusiva.

Sección 2

Cómo lograr que los procesos de elaboración de cibernormas incluyan a las partes interesadas marginadas y sus perspectivas.

Fase 1 Iniciativa

Se trata de la fase preparatoria de todo proceso de elaboración de normas, en la que las autoridades velan por garantizar la aceptación política, ultimar la visión estratégica de la normativa, establecer estructuras y procesos clave y determinar quiénes son las partes interesadas. En esta fase, las perspectivas de los grupos marginados deben integrarse en un proceso claro y sujeto a rendición de cuentas, acordado con las partes interesadas, para asesorar a las personas encargadas de la elaboración de las políticas y tomar decisiones en pie de igualdad. La clave es la transparencia y líneas de comunicación claras.

Qué hacer en esta fase

- **Realizar un mapeo inclusivo de las partes interesadas** para determinar cuáles son las comunidades a las que se debe escuchar y las que deben participar en el proceso. Un buen mapeo debe indicar los grupos marginados que pueden verse especialmente afectados por las ciberamenazas, así como las posibles soluciones para superar los obstáculos a su participación. En la **herramienta 1** se ofrece orientación detallada para lograrlo.
- **Establecer medidas proactivas para permitir la participación de grupos o personas marginadas.** Esto podría incluir, entre otras cosas:
  - **La publicación de plazos con suficiente antelación** para inscribirse en el proceso de participación y consulta.
  - **La admisión de aportes en formatos no escritos** (por ejemplo, testimonios orales, vídeos, fotografías, relatos biográficos o conversaciones estructuradas).
  - **La asignación de financiación y recursos materiales** a personas y grupos para que puedan participar, incluida la financiación para la conectividad de las TIC, para desplazamientos, alojamiento y manutención o para el cuidado de menores y personas ancianas.
  - **La traducción de los materiales** de los procesos normativos y de los procesos mundiales y regionales de carácter oficial de elaboración de cibernormas a todas las lenguas que requieran las partes interesadas. Del mismo modo, todos los aportes y propuestas de las múltiples partes interesadas deben traducirse a todos los idiomas oficiales de cada organización. Por ejemplo, para garantizar la contribución de las múltiples partes interesadas a las consultas sobre gobernanza mundial de las TIC y sobre las cibernormas en las Naciones Unidas, los materiales deben traducirse a los otros cinco idiomas oficiales de la Organización.
  - **La elaboración de rigurosos procedimientos** y directrices, en consulta con las partes interesadas, **para garantizar la privacidad y la protección** de todas las personas que participan en el proceso de elaboración de las normas, como la celebración de reuniones a puerta cerrada, el cumplimiento de la norma de Chatham House o la prestación de canales seguros para realizar aportes (mediante, por ejemplo, contribuciones anónimas o canales encriptados).
- **Establecer líneas claras de comunicación e información para que todas las personas estén al corriente de los avances**. Esto contribuirá a la transparencia y la rendición de cuentas durante el proceso. En aras de la participación constante, también puede considerarse un acuerdo sobre cómo tratar quejas, las disputas y los desacuerdos a lo largo del proceso (por ejemplo, cuando existan grandes divergencias políticas, pero también si no se cumplen determinados compromisos o hay casos de discriminación o marginación en el proceso normativo).

Otras consideraciones

- Consultar con las partes interesadas para averiguar qué forma de **capacitación y formación** les resultaría útil y provechosa, si procede, teniendo en cuenta que los patrones de discriminación también pueden reproducirse en la formación.
- Cultivar la **reflexión**. Cada cual debe reflexionar detenidamente sobre su posición social, sus prejuicios, sus posibles sesgos y su relación con las formas de poder y privilegio existentes, para evaluar de qué manera pueden estar influyendo en la toma de decisiones en esta fase.
- Prestar atención a **las jerarquías y las dinámicas existentes** entre las partes interesadas en los distintos sectores y dentro de ellos (por ejemplo, la sociedad civil y el sector privado). Es importante amplificar y dar cabida siempre a los aportes de los grupos habitualmente excluidos o marginados de los procesos de elaboración de cibernormas.
- Establecer un modelo y un **presupuesto** para compensar a las personas por su tiempo y su experticia en las consultas y las intervenciones de múltiples partes interesadas. De este modo, los procesos serán más colaborativos que extractivos.

Unos buenos resultados serían:

→ **Un mapeo** exhaustivo de las partes interesadas, acordada por quienes dirigen el proceso;
→ Contacto con un amplio abanico de partes interesadas de distintos grupos marginados;
→ Una visión común de lo que significa que el proceso normativo sea abierto, así como de los posibles obstáculos a la participación;
→ La definición de medidas proactivas para superar dichos obstáculos.

Fase 2 Evaluación y análisis

Una vez determinadas las partes interesadas, esta fase se centra en definir los aspectos en los que sus aportes serían especialmente útiles mediante un estudio y un análisis detallado del panorama normativo existente.

Qué hacer en esta fase

- **Entablar un diálogo permanente con los grupos identificados para comprender sus experiencias y puntos de vista**. Esto es importante para garantizar que el proceso sea transparente y esté sujeto a la rendición de cuentas. Llevará tiempo y exigirá un proceso continuo de intercambio de información sobre cómo reflejar o incorporar los aportes. No puede tratarse como un mero ejercicio administrativo. Las personas que participen en estos diálogos deben plantearse de qué manera sus identidades influyen en la disposición y la confianza de los demás participantes a compartir información.
- **Generar una visión común de cómo las cibernormas y, en particular, las ciberamenazas afectan a los grupos marginados y con marcadores específicos de género**, con los aportes de los grupos marginados determinados en el mapeo. Puede consistir en un documento de referencia o una nota conceptual en la que se describan y reflejen las repercusiones discriminatorias —incluidas de género y raza— de las ciberamenazas detectadas en contextos específicos. También puede incluir un análisis jurídico detallado de la normativa en cuestión mediante este planteamiento basado en la identidad, para detectar los riesgos específicos y concretos.
- **Demostrar iniciativa para obtener información de las partes interesadas**. No puede darse por sentado que basta con una petición general de aportes, sino que es preferible dirigirse directamente a los grupos marginados que se hayan identificado a través del mapeo de partes interesadas, teniendo en cuenta su capacidad y su participación previa. Esto es aún más importante cuando se solicitan aportes de grupos expuestos a grandes desventajas y que posiblemente carezcan de acceso a estructuras organizativas convencionales o a instituciones preexistentes.
- **Informar y mantener relaciones con las partes interesadas consultadas para compartir los resultados del análisis.** Es fundamental que los documentos sean accesibles y tengan en cuenta las distintas necesidades. Las partes interesadas deben estar al corriente de la evolución del proceso normativo y de si se están incluyendo sus puntos de vista y de qué manera. Además, deben tener la oportunidad de realizar observaciones sobre los borradores de los documentos.

Otras consideraciones

- Es clave reflexionar detenidamente sobre el modo en que las ideas de género, coloniales y raciales influyen en el proceso de creación de conocimientos dentro de la elaboración de normas.
- Las normas de conocimiento establecidas —y el lenguaje académico e institucional— pueden condicionar qué tipo de partes interesadas son percibidas como con más credibilidad.

Unos buenos resultados serían:

→ Las partes interesadas participan activamente en las conversaciones y manifiestan sentirse cómodas y satisfechas con su nivel de inclusión.

→ Existe una visión común acerca del efecto de las cibernormas en los grupos marginados y de género.

Fase 3 Elaboración de las normativas

Esta fase consiste en la redacción del texto en sí. Las partes interesadas deben participar en todas las fases del proceso de producción, pero su participación es particularmente importante en la revisión y las observaciones sobre los borradores del texto.

Qué hacer en esta fase

- Garantizar que **las partes interesadas identificadas participen** en el proceso de redacción y que las medidas establecidas en la fase 1 sigan siendo adecuadas.
- **Publicar los aportes al proceso de las partes interesadas.** Deben estar en un formato fácilmente accesible para todas las partes interesadas. Garantizar que las partes interesadas reciban un reconocimiento justo por sus contribuciones.
- Utilizar un **lenguaje accesible** y velar por que se atienda a las diferencias en el dominio de determinada terminología o registros lingüísticos (por ejemplo, es posible que ciertos grupos no estén familiarizados con la jerga académica). Esto es importante en aras de la apertura y la accesibilidad. Por ejemplo, si es necesario hacer aportes orales, es preciso asegurarse de que se transcriban con exactitud; deben asignarse fondos y tiempo para la traducción, sobre todo si se pretende llegar a comunidades marginadas que utilizan dialectos y lenguas locales diferentes.
- En aras de la transparencia, es fundamental asegurarse de que todos los **proyectos de texto tengan en cuenta las conclusiones y la experticia** recopilada durante la fase 2 y que se revisen periódicamente las repercusiones y perjuicios contra los grupos marginados que puedan derivarse del uso del lenguaje y la redacción. Comunicar a las partes interesadas el calendario y las modalidades de la fase de redacción y verificar que haya tiempo suficiente para revisar el texto y los aportes.
- **Programar revisiones y oportunidades para que todas las partes interesadas y agentes clave consultados participen y hagan aportes periódicamente** a lo largo de la fase de redacción, a fin de garantizar que los comentarios y la redacción sean un proceso iterativo.

Otras consideraciones

- El consenso es un objetivo importante y válido en la elaboración inclusiva de normativas. No obstante, también puede acabar reproduciendo el *statu quo*, con sus mismas estructuras de poder y prioridades, en función de la composición del grupo de múltiples partes interesadas y de cómo se interpreten y ejecuten los términos. Es imprescindible reexaminar los resultados del mapeo realizado para identificar a las partes interesadas y prestar especial atención a las jerarquías y dinámicas existentes entre ellas, para asegurarse de que la interpretación común de «consenso» sea realmente integradora.

Unos buenos resultados serían:

→ Una cibernorma que se haya elaborado o implementado de forma inclusiva, con una participación significativa de las partes interesadas marginadas.

→ Una cibernorma que, en su contenido, refleje de forma específica las necesidades y prioridades de todas las partes interesadas, incluidas las mujeres y los grupos marginados.

→ Una cibernorma que no perjudique a los grupos marginados ni acentúe las desigualdades a las que se enfrentan (por ejemplo, mediante auditorías de género o de inclusión).

Fase 4 Implementación

Cuando los grupos marginados y la sociedad civil participan en la elaboración de las normas y en el ajuste de los planes de acción que las acompañan, están más dispuestos a apoyar su implementación. La prioridad clave en esta fase es que la implementación y las funciones y responsabilidades pertinentes estén claras durante el periodo de implementación.

Qué hacer en esta fase

- En aras de la transparencia y la rendición de cuentas, es preciso elaborar un plan de implementación, con vías y etapas claras que articulen la participación de los grupos marginados. Debe incluir:
- Un calendario detallado, con información sobre el alcance de los aportes en cada punto;
- Revisiones periódicas de los avances, que brinden a las partes interesadas la oportunidad de aportar, examinar y plantear sus preocupaciones.
- Para garantizar la inclusividad a lo largo de todo el proceso, es necesario definir claramente las funciones y responsabilidades, las modalidades y las salvaguardias, de modo que los grupos marginados sigan implicados también en la implementación. Entre otras acciones, es necesario:
- Estudiar el posible impacto y repercusiones de la implementación de la norma;
- Crear, de manera colaborativa, mecanismos de transparencia y rendición de cuentas;
- Garantizar la participación activa de las partes interesadas y recopilar sus observaciones periódicamente para que la toma de decisiones sea ágil en todas las fases de implementación (esto podría solaparse con la fase de seguimiento y evaluación).

Otras consideraciones

- En la implementación debe garantizarse que el lenguaje en torno a la inclusión se integre en todo el ciclo de vida de las normativas. Esto podría lograrse, entre otros, garantizando que los equipos que se ocupan de la implementación —y, en particular, los equipos que generan las ideas— sean diversos e inclusivos, por ejemplo, mediante sistemas de cuotas y medidas directas para facilitar la participación de las comunidades afectadas. Esto también podría facilitarse mediante la asignación de recursos específicos a las personas con experiencia en el análisis interseccional de género responsables de proporcionar orientación técnica para garantizar la igualdad en la implementación.

Unos buenos resultados serían:

→ Un plan de aplicación detallado, con funciones y responsabilidades claramente definidas, plazos y medidas de rendición de cuentas y de comunicación para un que el intercambio de información sea transparente.

Fase 5 Seguimiento y evaluación

Esta etapa debe llevarse a cabo en paralelo a todas las demás. No basta con realizarla únicamente al final.

En esta fase, las partes interesadas marginadas deben ocupar un lugar central para garantizar una implementación inclusiva de las normas, y dar a conocer las deficiencias o lagunas de la legislación vigente que deben subsanarse para lograr la implementación de las cibernormas.

Qué hacer en esta fase

- **Elaborar un marco de medición de la inclusividad**, o una serie de parámetros de inclusividad, para evaluar si el proceso y la implementación de las cibernormas se llevan a cabo de forma inclusiva.
- **Establecer un grupo de trabajo multisectorial**, que incluya a representantes de las comunidades marginadas definidas y se encargue de coordinar y realizar los procesos de revisión.
- **Programar evaluaciones, revisiones y momentos de reflexión y análisis periódicos** a lo largo de todo el proceso normativo en los que participen todas las partes interesadas.
- **Responder de forma proactiva a los resultados de la evaluación e incorporar al proceso las lecciones aprendidas**, según proceda. Por ejemplo, cuando existan grandes divergencias políticas, pero también si no se cumplen determinados compromisos o si se dan casos de discriminación o marginación en el proceso normativo. Es crucial para garantizar que este sea transparente y esté sujeto a la rendición de cuentas.
- **Publicar las conclusiones y las lecciones aprendidas** para garantizar la rendición de cuentas y el intercambio de conocimientos entre diferentes comunidades, países y regiones.

Otras consideraciones

- Debe tenerse en cuenta que el seguimiento y la evaluación podrían dar lugar a un proceso de modificación de las normas, lo que podría requerir retomar el proceso desde la primera fase. Se trata de un ciclo constante y las normas no son inamovibles, por lo que hay que adoptar un enfoque reflexivo para reconocer si las conclusiones de la fase de evaluación avalan la necesidad de introducir modificaciones.

Unos buenos resultados serían:

→ Se acuerda un marco para la rendición de cuentas que incluya parámetros tangibles para evaluar los progresos realizados.

→ Se incorporan al proceso las lecciones extraídas de las revisiones programadas o periódicas y los momentos de reflexión o análisis.

Herramienta 1

Mapeo de las partes interesadas de forma inclusiva

En esta herramienta se ofrecen orientaciones detalladas para garantizar un enfoque rigurosamente integrador para el mapeo de partes interesadas. En términos generales, un enfoque integrador para la elaboración de cibernormas debe aspirar a una inclusión significativa de todas las partes interesadas, entre ellas:

1. las personas con un mandato, función o responsabilidad en el proceso;
2. las personas con las competencias o conocimientos necesarios para elaborar la política y ponerla en práctica;
3. las personas que podrían verse desproporcionadamente afectadas por la normativa o su aplicación, es decir, los grupos marginados.

Esta herramienta se centra en particular en las partes interesadas que podrían verse desproporcionadamente afectadas, y propone una serie de preguntas o indicaciones para las autoridades con responsabilidades normativas para que faciliten su participación en el proceso de elaboración de cibernormas. El objetivo consiste en ayudar a quienes elaboran las políticas a dejar de centrarse en las redes de instituciones y organizaciones preexistentes —que suelen tener mayor acceso al capital, el poder y los recursos— y comiencen a considerar de forma amplia y reflexiva el abanico de personas o grupos desproporcionadamente afectados por la elaboración de cibernormas.

Paso 1 Mapeo inicial de partes interesadas

Este primer paso está compuesto por una serie de preguntas orientadoras para ayudar a las personas encargadas de la formulación de políticas a realizar un mapeo inicial de las personas o grupos que podrían verse desproporcionadamente afectados por la formulación de cibernormas. El paso 1 está concebido como una evaluación preliminar basada en los conocimientos existentes, de las personas encargadas de elaborar la política, e investigación documental; debe ir seguido de una consulta efectiva y continua con las partes interesadas identificadas, como se indica en el paso 3.

Para maximizar su eficacia, las preguntas orientadoras que figuran a continuación deben responderse en relación con un proceso específico de elaboración de cibernormas: por ejemplo, la creación o implementación de una estrategia nacional de ciberseguridad o una política de ciberseguridad específica, como una política gubernamental de divulgación de vulnerabilidades, normas relativas a la protección de infraestructuras críticas o la creación de un centro nacional de respuesta a incidentes.

Preguntas orientadoras:

- ¿Cuáles son las cuestiones normativas que se pretenden resolver mediante el proceso de elaboración e implementación de las cibernormas?
- ¿A quién afectan, positiva o negativamente, las cuestiones normativas que se pretenden resolver?
- ¿Qué personas y grupos resultan afectados de forma específica y desproporcionada por estas cuestiones normativas? ¿Sufren consecuencias desproporcionadas debido a su identidad, condición o creencias?
- ¿Quién se ha beneficiado o perjudicado históricamente por los intentos de resolver estos problemas mediante la elaboración y aplicación de normativas? ¿Han sufrido un impacto desproporcionado debido a su identidad, condición o creencias?
- De los grupos señalados, ¿hay alguno que sufra las consecuencias de manera distinta por poseer características múltiples o que se entrecrucen?
- ¿Cuáles son las necesidades satisfechas y no satisfechas de los distintos grupos a los que se intenta responder mediante el proceso de elaboración de cibernormas?
- ¿Cómo podrían agravarse o remediarse las necesidades de los grupos mencionados como resultado de la aplicación de un determinado proceso de elaboración de cibernormas?
- ¿Qué organizaciones, grupos comunitarios u otras entidades trabajan en las cuestiones normativas antes mencionadas y relacionadas específicamente con la ciberseguridad? ¿Qué organizaciones, grupos o entidades trabajan en estos temas en relación con el género, la sexualidad y otras desigualdades?

Paso 2 Detección de los obstáculos

Las preguntas del paso 2 pretenden ayudar a quienes elaboran las políticas a considerar los obstáculos u otras sensibilidades que puedan ser un impedimento para que determinadas partes interesadas participen e intervengan de forma significativa en los procesos de elaboración de cibernormas.

La identificación de los obstáculos debe ser prioritaria en una fase temprana del proceso de mapeo y debe someterse a la validación y aportes de las partes interesadas definidas, tal y como se describe en el paso 3, para comprender cuáles son las barreras a las que es posible que se enfrenten y las distintas formas de adaptación que pueden necesitar. Estas preguntas requerirán respuestas específicas en función de los distintos grupos y es fundamental evitar las generalizaciones. Además de detectar los obstáculos, se anima a las autoridades normativas a velar por la inclusión de los grupos que no estén tan conectados u organizados oficialmente, así como de los que sí están mejor conectados y más formalmente constituidos; esto contribuirá a garantizar la inclusión de los grupos sin acceso a formas de capital social, poder y recursos.

Las preguntas orientadoras que figuran a continuación son pertinentes para cualquier proceso de participación de partes interesadas, aunque pueden requerir una mayor reflexión cuando se trabaja con grupos marginados, expuestos a patrones de discriminación sistémica.

En la fase 1 del conjunto de herramientas también se incluyen orientaciones adicionales para garantizar la participación de los grupos marginados.

Preguntas orientadoras:

- ¿Se organizan consultas en persona con suficiente antelación y a horas adecuadas del día?
- ¿Se realizan consultas y se distribuye el material normativo pertinente en los idiomas adecuados?
- ¿Se comunican las consultas con antelación para que las partes interesadas dispongan de tiempo suficiente para analizarlas y responder?
- ¿Se aceptan aportes en distintos formatos?
- ¿La comunicación es clara y comprensible para partes interesadas con distintas experiencias y conocimientos?
- ¿Resulta económicamente viable que las partes interesadas dediquen tiempo a participar en el proceso?
- ¿Es segura la participación de personas o grupos marginados, o sufrirán violencia o represión por expresar sus opiniones? Si no es así, ¿qué procesos alternativos pueden seguirse para facilitar su participación, como contribuciones anónimas o canales encriptados?
- ¿Los medios de participación son adecuados para las partes interesadas con tradiciones culturales diferentes?
- ¿Qué jerarquías y dinámicas pueden existir entre las partes interesadas que deban tenerse en cuenta?

Paso 3 Revisión y consulta

Tras la identificación inicial de las partes interesadas y los posibles obstáculos en los pasos 1 y 2, se anima a las autoridades normativas a establecer contacto con las partes interesadas identificadas y a consultarles sobre los resultados de su mapeo inicial. El tercer y último grupo de preguntas es una serie de sugerencias que las autoridades normativas deben formular a las partes interesadas identificadas.

En este paso, las autoridades deben solicitar aportes de forma activa y abierta para detectar cualquier laguna en su mapeo y determinar si falta alguna parte interesada que deba participar. Las autoridades normativas también deben tratar de comprender mejor los obstáculos y las sensibilidades detectadas, así como las adaptaciones que puedan ser necesarias para que las partes interesadas participen e intervengan de forma significativa en el proceso de elaboración de normas. Esta consulta debe ser efectiva, con aportes que sirvan realmente para ampliar o ajustar el mapeo.

Preguntas orientadoras:

- ¿El mapeo de las cuestiones normativas en juego y su repercusión en los distintos grupos marginados es preciso y está actualizado? ¿Existe algún efecto negativo (o positivo) que no se haya detectado, o algún grupo desfavorecido que no se haya tenido en cuenta?
- ¿El mapeo de las necesidades de los distintos grupos marginados y la forma en que estas pueden agravarse o remediarse a través del proceso de elaboración de políticas es preciso y completo? ¿Existe alguna posible consecuencia que no se haya tenido en cuenta?
- ¿Se ha tenido en cuenta en el mapeo la situación de las partes interesadas que sufran consecuencias de manera distinta por poseer características múltiples o que se entrecrucen?
- ¿Los grupos, entidades u organizaciones comunitarios incluidos en el mapeo son representativos de diversas identidades y perspectivas? ¿Hay grupos o perspectivas que no estén adecuadamente representados? ¿Quién más debería participar?
- ¿El mapeo de las barreras y otras sensibilidades experimentadas por los diferentes grupos marginados es preciso y completo? ¿El mapeo es específico para determinados grupos y evita las generalizaciones?
- ¿Qué ajustes deberían realizarse para garantizar su participación y compromiso efectivos en el proceso de elaboración de normas?

Esta herramienta se ha basado en los conocimientos y el enfoque expuestos en: The Centre for Feminist Foreign Policy, ***The Intersectionality and Cybersecurity Toolkit***, Marissa Conway y Nehmat Kaur, marzo de 2022.

Herramienta 2

Glosario de género e inclusión

En este anexo se incluye una introducción a los términos y conceptos clave en los que se basa la elaboración inclusiva de normas con múltiples partes interesadas. Dado que la terminología relativa a la igualdad, las comunidades marginadas y la identidad puede variar de un contexto a otro, este resumen conceptual debe interpretarse de la forma más amplia e inclusiva posible.

Género

Por «género» se entienden los roles, los comportamientos y los valores establecidos social y culturalmente que se asocian a la masculinidad y la feminidad en una época y un lugar determinados. Las normas de género evolucionan con el tiempo; determinan las identidades individuales, las relaciones sociales y la distribución de los recursos y el poder en la sociedad. Si bien el género suele entenderse como la expresión de las expectativas sobre la conducta que se considera adecuada en los hombres y en las mujeres, el género no es binario. Es diverso. Hace referencia a personas de todas las identidades y expresiones de género. Por tanto, se entiende por igualdad de género la igualdad de derechos, oportunidades y resultados para los hombres, las mujeres, las niñas, los niños y las personas de diversas identidades y expresiones de género. La igualdad de trato sin distinción por motivos de género es un derecho humano consagrado en el derecho internacional.

Identidad de género

La identidad de género es la concepción íntima que cada persona tiene de su propio género. Para algunas personas, denominadas cisgénero, esta coincide con el sexo que se les asignó al nacer. «Trans» es un término genérico que hace referencia a las personas cuya identidad de género no concuerda o no coincide con el sexo/género que se les asignó al nacer. Las identidades trans son diversas y a menudo específicas en términos sociales, regionales y culturales. Las identidades trans diversas pueden incluir, entre otras, las identidades no binarias, de género fluido, transgénero agénero, de tercer género y/o queer. Los hombres transgénero son personas a las que se les asignó sexo femenino al nacer, pero que son hombres y viven y se identifican como tal. Las mujeres transgénero son personas a las que se asignó un sexo masculino al nacer, pero que son mujeres y viven y se identifican como tal.

Expresión de género

La expresión de género es la forma en que las personas expresan y viven su género a través de sus acciones y aspecto. Las personas cuya expresión de género no se corresponde con las expectativas sociales (normalmente derivadas de las expectativas binarias de masculinidad y feminidad heterosexuales) también pueden sufrir estigmatización, discriminación y violencia,

al igual que las personas con identidades de género diversas. Por lo tanto, es imprescindible tener en cuenta a las personas de diversas sexualidades e identidades y expresiones de género en todos los aspectos de la elaboración de políticas, desde la participación de múltiples partes interesadas hasta el contenido sustantivo de las normas.

Orientación Sexual

La orientación sexual se refiere a la atracción emocional, física y romántica de una persona hacia otras. Si bien la sexualidad suele entenderse en términos de **heterosexualidad** (atracción por personas del llamado «sexo opuesto») y **homosexualidad** (atracción por personas del llamado «mismo sexo»), la sexualidad tampoco es binaria, sino que es diversa. Pese a que la sexualidad es independiente del género, la heterosexualidad suele ser una de las grandes expectativas de género tanto para los hombres como para las mujeres, y puede acarrear experiencias de estigmatización, discriminación y violencia para las personas de orientaciones sexuales distintas. Por lo tanto, es primordial considerar conjuntamente la sexualidad y el género en todos los aspectos del proceso de elaboración de políticas, incluida la representación, pero sin limitarse a ella.

Esencialismo

El esencialismo es una concepción sobre el género (y la identidad en general) que parte de la base de que la identidad, la expresión y, a menudo, los objetivos, los valores y la trayectoria vital del género se derivan directamente de una concepción binaria y biológica del sexo. Por lo tanto, el esencialismo también asume que todos los hombres y todas las mujeres tienen necesidades, capacidades y deseos idénticos entre sí. Las actitudes de género esencialistas también tienden a hacer caso omiso o a negar las capacidades, los deseos, las necesidades e incluso la existencia de personas con identidades y expresiones de género y orientaciones sexuales diversas. El esencialismo se manifiesta a menudo en la creación y el análisis de políticas en forma de **estereotipos de género** y pensamiento binario. Entre otras creencias, se asume, por ejemplo, que las mujeres son pasivas, emocionales y quieren ser madres, mientras que los hombres son agresivos, racionales y se dedican principalmente a actividades económicas formales.

Interseccionalidad

La interseccionalidad es un concepto -y una lente analítica- que refleja las múltiples formas de poder social vinculadas a la clase, la raza, la colonialidad, la nacionalidad, la capacidad, la etnia, la casta, la orientación sexual, la edad, la ubicación geográfica, la expresión de género, etc., que, junto con el género, generan patrones de marginación y exclusión.

El término fue acuñado por Kimberlé Crenshaw, profesora de Derecho estadounidense, sobre la base de una larga tradición del feminismo afroamericano. Las perspectivas interseccionales entienden que la marginación y la opresión no son la suma aditiva de distintas formas de discriminación (por ejemplo, género + raza + clase). Al contrario, se entiende que la marginación y la discriminación se experimentan de forma simultánea y específica, en un principio, como mujeres afrodescendientes de Estados Unidos.

Siguiendo este legado, la «interseccionalidad» va más allá de las ideas de inclusividad y diversidad (e incluso de demografía) para analizar las dinámicas de poder y las jerarquías sociales que generan estos patrones y experiencias de marginación y discriminación. Un potente

precursor del cambio social es afrontar la expresión y el mantenimiento de las diferentes formas de poder (por ejemplo, el patriarcado, la desigualdad de clases, la supremacía blanca, el colonialismo, el capacitismo, la heteronormatividad, la cisnormatividad, etc.) en los sistemas e instituciones sociales. Al igual que la elaboración de cibernormas, la interseccionalidad es un proceso continuo más que un objetivo final en sí mismo.

Grupos marginados

Al hablar de grupos marginados, se hace referencia a los grupos que carecen de poder. La marginación suele ser un efecto de la discriminación sistémica e histórica, que puede desembocar en la exclusión de grupos o comunidades enteros. En el derecho internacional se recoge una lista larga y abierta de más de treinta motivos de discriminación. Si bien la marginación es a menudo consecuencia de la discriminación, no todas las personas expuestas a ella pueden calificarse necesariamente de marginadas. Existen desigualdades en todos los lugares, pero su expresión específica y a quién afectan difiere de un lugar a otro. Por lo tanto, es importante trabajar con los agentes de la sociedad civil para comprender cómo funciona la marginación en cada contexto específico, en lugar de partir de ideas preconcebidas. Así es como se pasan por alto algunos aspectos de la marginación y las necesidades y perspectivas de comunidades concretas.

Feminismo

El feminismo es un compromiso amplio con la promoción de la igualdad de género y la lucha contra la desigualdad entre mujeres, hombres y personas de identidades, expresiones y orientaciones sexuales diversas. A través de una lente interseccional, el feminismo hace hincapié en el género y la sexualidad como formas de poder y estructuras sociales que fundamentan la vida social, económica y política. El feminismo en la elaboración de políticas implica un compromiso con la igualdad, la colaboración, el diálogo abierto y la solidaridad interseccional. El feminismo entiende que el proceso de elaboración, implementación y evaluación de las normas es un espacio tan importante para la defensa y el cambio como los propios resultados de las normas que se elaboren.

Herramienta 3

Mapeo de procesos de elaboración de cibernormas

La elaboración de normas voluntarias no vinculantes para el comportamiento de los Estados en materia de ciberseguridad internacional comenzó hace más de una década. Los procesos multilaterales de elaboración de normas cibernéticas se concibieron como vías puramente intergubernamentales, si bien se están abriendo cada vez más a la participación de diversos agentes no gubernamentales en el establecimiento, la puesta en práctica y la aplicación de las normas.

La elaboración de cibernormas, en sus diversas vías, es una actividad en constante evolución. Pueden surgir nuevos espacios con el tiempo y cuando se renueven los mandatos de los procesos existentes, como el Grupo de Trabajo de Composición Abierta (GTCA) sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional. La diversificación del panorama normativo y la aparición de agentes no estatales como artífices de normas ha creado aún más oportunidades para que la sociedad civil, incluidas las mujeres y los grupos marginados, participen en estos procesos. Su participación es fundamental, en particular, para incorporar las consideraciones de género a los esfuerzos de elaboración de cibernormas; además, las posibilidades y modalidades de participación están evolucionando en los foros existentes.

En este documento explicativo se pretende mapear los distintos procesos de elaboración de cibernormas y ayudar a identificar los foros clave y las posibles vías de participación e influencia, en particular para las organizaciones que representan a las mujeres y a las comunidades marginadas. Cuando procede, la información sobre los procesos en curso se ofrece en el contexto de los acontecimientos pasados que determinaron las actividades presentes de elaboración de normas.

El mapeo se estructura en función del nivel al que se realiza la actividad —nacional e internacional— y de la naturaleza de las partes interesadas que dirigen el proceso. La atención se centra principalmente en los procesos que entienden las cibernormas como compromisos voluntarios y no vinculantes, en contraposición a los tratados y obligaciones vinculantes. Sin embargo, se ha incluido información sobre esos instrumentos y marcos vinculantes cuando están estrechamente relacionados con la ciberseguridad internacional. Este es un resumen general de los procesos de elaboración de cibernormas más relevantes y no debe considerarse una lista exhaustiva.

1. Nivel internacional

1.1. Vías multilaterales internacionales: Naciones Unidas

1.2. Otros procesos gubernamentales de carácter internacional

1.3. Procesos internacionales no gubernamentales

2. Nivel regional

2.1. Organizaciones intergubernamentales regionales

2.2. Organización de Estados Americanos (OEA)

2.3. Asociación de Naciones del Sudeste Asiático (ASEAN)

2.4. Unión Africana (UA)

2.5. Organización para la Seguridad y la Cooperación en Europa (OSCE)

2.6. Unión Europea (UE)

2.7. Organización de Cooperación de Shanghai (OCS)

1. Nivel Internacional

1.1. Vías multilaterales internacionales: Naciones Unidas

Primera Comisión de las Naciones Unidas: normas no vinculantes, ciberseguridad internacional

Los procesos de elaboración de cibernormas en las Naciones Unidas comprenden dos vías que tratan la ciberseguridad internacional y la conducta responsable de los Estados en el ciberespacio: el Grupo de Expertos Gubernamentales (GEG) sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional y el Grupo de Trabajo de Composición Abierta (GTCA) sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional. Los mandatos de ambos grupos dependen de la Primera Comisión de la Asamblea General de las Naciones Unidas, que se ocupa de las amenazas a la paz y la seguridad internacionales. Si bien el proceso del GTCA comenzó transcurridos más de diez años desde el establecimiento del primer GEG, los resultados de sus respectivas tareas están interrelacionados y, en cierta medida, se refuerzan mutuamente.

Grupo de Expertos Gubernamentales (GEG) sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional

El proceso del GEG comenzó en 2004. Entre 2004 y 2021, el grupo celebró seis rondas de negociación, y cuatro de ellas concluyeron con informes de consenso. Los resultados de cada reunión del GEG se basaron en el trabajo anterior y proporcionaron hitos importantes para la elaboración e implementación de normas cibernéticas.

El primer informe de consenso del GEG, de 2010, reconoce la necesidad de que los Estados se pusieran de acuerdo sobre las normas de conducta responsable en el ciberespacio. Sin proponer ninguna norma, recomendó entablar un diálogo sobre la cuestión. Tres años después, en la siguiente ronda de negociaciones del GEG, se llegó a la conclusión de que el marco jurídico internacional existente permite derivar algunas normas, como la aplicación de la soberanía estatal en el ciberespacio y la protección de los derechos humanos, al tiempo que se tratan cuestiones de seguridad.

El resultado más importante del trabajo del GEG se obtuvo en 2015, cuando el grupo acordó once normas no vinculantes. Si bien no se impusieron obligaciones vinculantes a los Estados, en esas normas voluntarias se establecen una serie de pautas acordadas en términos generales sobre la conducta que se espera de estos en el ciberespacio. Esto implica tanto comportamientos positivos que se deben promulgar como comportamientos negativos de los que los Estados deben abstenerse. Entre las normas figuran:

a. la cooperación entre los Estados para elaborar y aplicar medidas que encaminadas a mejorar la seguridad y la estabilidad en el uso de las tecnologías de la información y las comunicaciones y la prevención de prácticas nocivas en este ámbito;
b. el examen de toda la información pertinente en caso de incidentes relacionados con las tecnologías de la información y las comunicaciones;
c. la expectativa de que los Estados velen por que no se utilice su territorio para cometer hechos internacionalmente ilícitos mediante las tecnologías de la información y las comunicaciones;

d. la cooperación para combatir el uso de las tecnologías de la información y las comunicaciones con fines delictivos y terroristas;
e. el respeto de los derechos humanos y de la intimidad para garantizar un uso seguro de las tecnologías de la información y las comunicaciones;
f. la expectativa de no realizar o apoyar con conocimiento de causa actividades relacionadas con las tecnologías de la información y la comunicación que dañen infraestructuras fundamentales;
g. el compromiso de los Estados a adoptar las medidas adecuadas para proteger sus infraestructuras fundamentales;
h. el compromiso de responder a las solicitudes de asistencia pertinentes de otro Estado cuyas infraestructuras fundamentales sean objeto de actos con fines malintencionados relacionados con las tecnologías de la información y la comunicación;
i. la verificación de la integridad de la cadena de suministro y prevenir la proliferación de instrumentos y técnicas malintencionados que tengan funciones dañinas ocultas en relación con las tecnologías de la información y la comunicación;
j. el fomento del intercambio de información sobre las vulnerabilidades de las tecnologías de la información y la comunicación; y
k. el compromiso de no perjudicar el trabajo de los equipos de respuesta a emergencias autorizados y de no autorizar la participación de los equipos de respuesta a emergencias en actividades malintencionadas.

Tras la aprobación de la resolución 70/237 de la Asamblea General de las Naciones Unidas, en la que se exhorta a los Estados Miembros a guiarse por el informe del Grupo de Expertos Gubernamentales en su uso de las tecnologías de la información y las comunicaciones, las once normas se han convertido en una referencia para otros procesos relacionados con la ciberseguridad internacional, como los esfuerzos de fomento de la confianza y creación de capacidades por parte de las organizaciones regionales. No obstante, en la siguiente ronda de negociaciones del GEG, celebrada en 2016-2017, resultó imposible aprovechar este avance y se estancó el proceso, ya que los Estados no lograron llegar a un acuerdo sobre la aplicabilidad del derecho internacional en el ciberespacio.

Tras esta falta de consenso en el GEG, la Asamblea General de las Naciones Unidas adoptó dos resoluciones contradictorias. En virtud de una de ellas, se convocó el siguiente período de sesiones del GEG —el sexto—, mientras que en otra se establecía un proceso novedoso: un Grupo de Trabajo de Composición Abierta (GTCA). A diferencia del carácter exclusivo del GEG, que inicialmente estaba compuesto por 15 países y aumentó a 25 miembros en 2016, sin la participación de otros Estados miembros o partes interesadas en sus reuniones, el GTCA estaba abierto a todos los Estados Miembros interesados. Las dos vías deliberaron en paralelo entre 2019 y 2021. En mayo de 2021, en el sexto informe de consenso del GEG, se reafirmaron las once normas del informe de 2015 y se trató de mejorar su interpretación y aplicación.

Grupo de Trabajo de Composición Abierta (GTCA) sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional

El GTCA 2019-2021 llegó a un consenso en marzo de 2021. En su informe final se incluían recomendaciones en relación con las reglas, normas y principios de conducta responsable de los Estados en el ciberespacio, la aplicabilidad del derecho internacional, las medidas de fomento de la confianza y otras cuestiones. En la segunda parte de los resultados del GTCA, el resumen del Presidente, se recogían las cuestiones sobre las que no se había llegado a un consenso y se pretendía que sirvieran de base para futuras deliberaciones sobre cibernormas.

Tercera Comisión de la Asamblea General de las Naciones Unidas: Tratado vinculante, delincuencia y justicia penal

Además de los procesos relacionados con las normas cibernéticas de la Primera Comisión de la Asamblea General, existe otro órgano en las Naciones Unidas, el Comité Especial encargado de Elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos, que se ocupa actualmente de la ciberdelincuencia. A diferencia del concepto de cibernormas, cuyo objetivo es crear compromisos no vinculantes, se espera que las negociaciones del Comité Especial desemboquen en un tratado vinculante. Tras su establecimiento con arreglo a la resolución 74/247 de la Asamblea General de las Naciones Unidas, el Comité Especial sobre Ciberdelincuencia comenzó su trabajo en 2021 con miras a adoptar el tratado en febrero de 2024.

1.2. Otros procesos gubernamentales de carácter internacional

Si bien las Naciones Unidas siguen siendo la vía más importante de participación en los principales procesos mundiales de elaboración de normas cibernéticas, tras la aprobación del informe de 2015 del GEG, surgieron varias iniciativas internacionales. Algunas tomaron las once normas como base para su trabajo, y otras crearon sus propios compromisos voluntarios. Entre estas iniciativas figuran organizaciones multilaterales, como el **Grupo de los Siete (G7)**, asociaciones políticas como la **Commonwealth**, y procesos establecidos por los gobiernos que adquirieron magnitud internacional, como el **Llamamiento de París**.

Las once normas recogidas en el informe del GEG de 2015 son el pilar de los compromisos de varios foros multilaterales. El Comunicado del **Grupo de los 20 (G20)** en Antalya reconoció el papel clave del GEG en la elaboración de las normas de conducta estatal responsable en el ciberespacio y suscribió las once normas del informe del GEG de 2015. Del mismo modo, el **Grupo de los Siete (G7)**, en su Declaración sobre la Conducta Responsable de los Estados en el Ciberespacio 2017, apoyó la promoción de normas cibernéticas voluntarias e hizo referencia a las once normas del informe de 2015 del GEG y al Comunicado del G20 que las respaldó. El Informe del Presidente de la Reunión del Grupo Cibernético del G7 en Ise-Shima destaca, además, el compromiso del Grupo de los Siete de seguir trabajando con las partes interesadas gubernamentales y no gubernamentales en la elaboración de normas cibernéticas no vinculantes. Este compromiso se materializó en la Declaración de Dinard del G7, donde se estableció la Iniciativa sobre Cibernormas (CNI) para compartir las prácticas óptimas en la aplicación de las normas reconocidas.

La **Commonwealth**, en su declaración sobre cuestiones cibernéticas de 2018, se comprometió a promover normas voluntarias para una conducta estatal responsable y a formular medidas de fomento de la confianza acordes con las normas del informe de 2015 del GEG. Esta se está poniendo en práctica mediante el Programa de Ciberseguridad de la Commonwealth.

La **Coalición por la Libertad en Línea (FOC)** es una asociación de 37 gobiernos que trabajan codo a codo para promover la libertad en Internet. En los últimos años, la FOC ha emitido varias declaraciones conjuntas, así como recomendaciones relacionadas con la ciberseguridad. Por ejemplo, sus recomendaciones para adoptar un enfoque de la ciberseguridad basado en los derechos humanos representan un compromiso de los Estados Miembros de la FOC para abordar la ciberseguridad desde el punto de vista de los derechos humanos.

El Gobierno de Francia lanzó en 2018 el **Llamamiento de París para la Confianza y la Seguridad en el Ciberespacio**. El Llamamiento es un compromiso para mantener la paz y la estabilidad en el ciberespacio, y comprende nueve principios: proteger a las personas y las infraestructuras, proteger Internet, defender los procesos electorales, defender la propiedad intelectual, la no proliferación, la seguridad del ciclo de vida, la ciberhigiene, la no piratería privada y las normas internacionales. A pesar de ser una iniciativa gubernamental, estos compromisos se dirigen tanto a los agentes estatales como a los agentes no estatales, a diferencia de las normas del GEG, que se centran en los Estados. Algunos de los principios, como la protección de las infraestructuras, se solapan con las normas del GEG de las Naciones Unidas y pueden considerarse una forma de poner en práctica la labor del GEG. Otros constituyen nuevos compromisos público-privados en materia de ciberseguridad. En agosto de 2022, el llamamiento contaba con el apoyo de 81 gobiernos, 390 organizaciones de la sociedad civil y 706 entidades del sector privado.

1.3. Procesos internacionales no gubernamentales

Mientras que los primeros procesos normativos cibernéticos, como el GEG, constituían un diálogo interestatal y alumbraban compromisos voluntarios por y para los gobiernos, en los últimos años, los esfuerzos normativos son cada vez más plurales. Cuando resulta complicado lograr el consenso entre los gobiernos debido a tensiones políticas, la actuación de las partes interesadas no gubernamentales puede complementar la labor intergubernamental y ofrecer una vía alternativa para lograr un ciberespacio más estable y seguro. La elaboración y aplicación de cibernormas por parte de agentes no estatales ha ampliado el concepto mismo de cibernormas, que ha pasado de ser sinónimo de compromisos interestatales voluntarios a convertirse en promesas prácticas de diversas partes interesadas.

Procesos impulsados por el sector privado

La participación del sector privado en el debate sobre las cibernormas comenzó en 2017 con una propuesta de «Convención Digital de Ginebra» que presentó Microsoft. La propuesta pedía a los Estados que se comprometieran a cumplir varias normas, como limitar su participación en ciberataques y en la proliferación de ciberarmas. Esta iniciativa recibió críticas por centrarse únicamente en las responsabilidades de los Estados, sin tener en cuenta la existencia de diversas vías para desarrollar las normas de conducta estatal responsable. Para hacer extensivo estos compromisos al sector privado, Microsoft estableció el **Cybersecurity Tech Accord** en 2018. Este acuerdo propone varios principios dirigidos al sector privado para proteger a los usuarios, reforzar la ciberseguridad y desarrollar alianzas en este ámbito. En agosto de 2022, ya habían suscrito el acuerdo más de 150 empresas.

Otro esfuerzo del sector privado dirigido a la elaboración de cibernormas, la **Carta de Confianza**, llegó de la mano de Siemens en la Conferencia de Seguridad de Múnich de 2018. Esa Carta contiene diez principios dirigidos principalmente al sector industrial y, hasta la fecha, 17 empresas privadas se han comprometido a cumplirlos.

Otros procesos

La **Global Commission on Stability in Cyberspace (GCSC)** se creó en febrero de 2017 y estaba formada por 26 comisionados de diversas regiones geográficas y grupos de partes interesadas. A partir del trabajo del GEG, en el informe final de la GCSC se proponen cuatro principios

(responsabilidad, moderación, obligación de actuar y respeto de los derechos humanos) y ocho normas para los agentes estatales y no estatales.

La iniciativa de **normas mutuamente acordadas para la seguridad de enrutamiento (MANRS)** de Internet Society presenta un conjunto voluntario de compromisos técnicos (medidas) para mejorar la seguridad del enrutamiento. Se lanzó en 2014 con cuatro compromisos para los operadores de redes. En 2018 se amplió con el programa para puntos de intercambio de Internet y, en 2020, con los programas para las redes de distribución de contenidos y la nube.

2. Nivel Regional

Organizaciones intergubernamentales regionales

Las organizaciones intergubernamentales regionales desempeñan una función clave en la aplicación de las normas del GEG de las Naciones Unidas, en ocasiones a través de sus propios procesos de formulación de normas cibernéticas. Los esfuerzos regionales de organizaciones, como la Organización de Estados Americanos (OEA), la Organización para la Seguridad y la Cooperación en Europa (OSCE), la Unión Africana (UA) y otras, pueden revestir una mayor legitimidad institucional entre sus miembros, ofrecer una mejor comprensión del contexto cultural e histórico y de las prioridades regionales, y facilitar la cooperación y el desarrollo de capacidades adaptados a su región.

Organización de Estados Americanos (OEA)

La OEA fue la primera organización regional en reconocer la necesidad de fomentar la confianza en el ciberespacio: la referencia a las medidas de fomento de la confianza puede encontrarse en la declaración de 2009 de la Comisión de Seguridad Hemisférica de la OEA. La OEA elaboró su primer conjunto de medidas de fomento de la confianza en materia de ciberseguridad en 2018 con el objetivo de fomentar el intercambio de información entre los agentes estatales. Al año siguiente, en 2019, su propuesta en la materia se centró en la diplomacia cibernética y el desarrollo de capacidades. Las últimas medidas publicadas en 2020 incluían 31 medidas «tradicionales» y «no tradicionales» que abarcaban un amplio abanico de cuestiones relacionadas con la cooperación en materia de ciberseguridad. En particular, una de las medidas tradicionales prevé la participación de los agentes no estatales, en particular la sociedad civil, en la difusión y el debate de las medidas de fomento de la confianza.

Asociación de Naciones del Sudeste Asiático (ASEAN)

Los Estados miembros de la ASEAN se comprometieron en 2016 a elaborar un conjunto de normas en materia de ciberseguridad para la región. En 2018, los ministros de la ASEAN acordaron suscribir «en principio» las normas del informe de 2015 del GEG, y los mandatarios de la ASEAN expresaron por separado su compromiso de convertir la operatividad de las normas del GEG en la piedra angular del enfoque regional de la ASEAN para la estabilidad en el ciberespacio. La aplicación práctica del informe de 2015 del GEG es uno de los pilares principales del Proyecto de Estrategia de Cooperación en Ciberseguridad 2021-2025 de la ASEAN. En esa estrategia se recogen las medidas concretas esbozadas por la ASEAN, incluida la importancia de la capacitación de las múltiples partes interesadas, con referencia a los informes del GEG y del GTCA (2021).

Unión Africana (UA)

La Unión Africana ha adoptado medidas muy limitadas para suscribir las normas incluidas en el informe de 2015 del GEG y para fomentar enfoques regionales en materia de formulación de cibernormas. Si bien la Estrategia de Transformación Digital para África 2020-2030 propone apoyar los procesos de ciberseguridad liderados por las Naciones Unidas, el enfoque de la UA en materia de ciberseguridad se centra más en la ciberdelincuencia. En 2014, la UA adoptó el Convenio sobre Ciberseguridad y Protección de Datos, un instrumento jurídicamente vinculante. No obstante, a fecha de agosto de 2022, el Convenio todavía no había entrado en vigor, ya que solo lo habían ratificado 13 estados de los 15 necesarios. Algunos investigadores cuestionan incluso que las cibernormas del informe de 2015 del GEG se hayan hecho a la medida de los estados del continente africano, dado que en ellos no se originan las cadenas de suministro y algunos países carecen de capacidad para responder a los incidentes.

Organización para la Seguridad y la Cooperación en Europa (OSCE)

La formulación de cibernormas en la OSCE se centra en el fomento de la capacidad y la confianza. Desde 2013, la OSCE ha desarrollado dos conjuntos de medidas de fomento de la confianza (MFC). El primer conjunto, elaborado en 2013, preveía el establecimiento de puntos de contacto y canales de comunicación, y el segundo (2016), tenía por objeto lograr una mayor previsibilidad, potenciar las comunicaciones y mejorar la preparación. En 2016, la OSCE inició un proyecto para afrontar las dificultades que plantea la aplicación de las medidas de fomento de la confianza en cooperación con el Foro Global sobre Experticia Cibernética (GFCE) y otros asociados. Recientemente, en la Declaración de Birmingham 2022 de la OSCE, se instaba a los Estados a abstenerse de realizar actividades malintencionadas en el ciberespacio y de vulnerar los derechos humanos, y se pedía una mayor aplicación de las medidas de fomento de la confianza.

European Union (EU)

La Unión Europea ha participado activamente en los debates del GEG y del GTCA y ha expresado su apoyo y compromiso constantes con las once normas del informe de 2015 del GEG. En la política de ciberseguridad de la Unión Europea se aplican muchos aspectos de las normas del GEG a través de diversos instrumentos, entre ellos distintas normativas y estrategias y varios instrumentos vinculantes, como el conjunto de herramientas de ciberdiplomacia, la Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad, el Reglamento sobre la Ciberseguridad y muchos otros.

Organización de Cooperación de Shanghái (OCS)

La OCS tiene una visión muy diferente de la ciberseguridad, puesto que entienden como la «seguridad de la información»; en las negociaciones de las Naciones Unidas, las posturas de sus miembros han defendido la idea de que los Estados tienen derecho a controlar la información dentro de sus fronteras. En 2011, algunos miembros de la OCS (China, Rusia, Tayikistán y Uzbekistán) propusieron a la Asamblea General de las Naciones Unidas un «Código Internacional de Conducta para la Seguridad de la Información». Ese Código recibió críticas por su ambigüedad, su fuerte dependencia de los conceptos de seguridad nacional y su posible impacto en la libertad de expresión y otros derechos humanos. La versión actualizada

del Código, presentada en 2015, se centraba en la igualdad de derechos entre los Estados y en la importancia de la gobernanza de Internet. Tanto la propuesta de 2011 como la de 2015 sugieren que el Internet debería gobernarse de forma multilateral, frente al modelo actual de múltiples partes interesadas.