Documento final del itinerario parlamentario
17.ª reunión del Foro para la Gobernanza de Internet de las Naciones Unidas

Abordar las ciberamenazas: enfoques nacionales, regionales e internacionales

1 de diciembre de 2022

Nosotros, los parlamentarios participantes en el itinerario parlamentario de la 17.ª reunión del Foro para la Gobernanza de Internet de las Naciones Unidas,

Reuniéndonos en el contexto de la 17.ª reunión del Foro para la Gobernanza de Internet (IGF) de las Naciones Unidas y debatiendo cuestiones relacionadas con los enfoques nacionales, regionales e internacionales –estatales, multilaterales y multisectoriales– para abordar las ciberamenazas,

Acogiendo con beneplácito la continuación y el fortalecimiento del itinerario parlamentario del IGF, y basándonos en las recomendaciones de las ediciones de 2019, 2020 y 2021 de que los parlamentos nacionales cooperen e intercambien buenas prácticas a la hora de abordar cuestiones de política digital,

Reconociendo la función del Departamento de las Naciones Unidas de Asuntos Económicos y Sociales (ONU DAES), la Unión Interparlamentaria (UIP) y la Cámara de Representantes del Pueblo de Etiopía en la coorganización del itinerario parlamentario del IGF 2022, así como el apoyo proporcionado por la Secretaría del IGF,

Recordando la resolución 74/304 del 9 de septiembre de 2020 de la Asamblea General de las Naciones Unidas, que alienta a las Naciones Unidas, a los parlamentos nacionales y a la Unión Interparlamentaria a que fortalezcan la cooperación,

Tomando nota de los informes del Secretario General de las Naciones Unidas *Hoja de ruta para la cooperación digital* y *Nuestra Agenda Común*, que ponen de relieve la importancia de fortalecer la cooperación de múltiples interesados para garantizar la seguridad en línea,

Señalando que, aunque Internet y las tecnologías digitales van teniendo un protagonismo cada vez mayor a la hora de configurar nuestras economías y sociedades, también pueden crear vulnerabilidades para las personas, las entidades públicas y privadas, las infraestructuras críticas y mucho más,

Recordando que la “ciberseguridad” y la “ciberdelincuencia” son cuestiones relacionadas aunque distintas, ya que la “ciberseguridad” es un aspecto que debe mejorarse y la “ciberdelincuencia” algo que debe impedirse,

Apuntando la importancia de instrumentos internacionales como el Convenio sobre la Ciberdelincuencia (Convenio de Budapest) del Consejo de Europa, en el que hay actualmente 68 Estados Partes, y de instrumentos regionales como la Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales (Convención de Malabo), así como la función que pueden desempeñar ese tipo de instrumentos para impulsar la cooperación internacional y regional,

Reconociendo que nunca faltan las preocupaciones geopolíticas en los debates sobre ciberseguridad, ratificando a su vez que todos los países comparten el interés común de mejorar la ciberseguridad y combatir la ciberdelincuencia,

Reconociendo igualmente que el panorama cibernético es complejo y que los países tienen diferente grado de preparación para abordar las ciberamenazas,

Señalando que las cuestiones de la ciberseguridad y la ciberdelincuencia tienen dimensiones interinstitucionales y transfronterizas, y que su abordaje requiere:

a) Enfoques en todo el Gobierno y en toda la sociedad que conlleven asociaciones sólidas y esfuerzos coordinados entre las autoridades y agencias competentes, el sector privado, la comunidad técnica, el mundo académico y la sociedad civil,
b) Una cooperación regional e internacional que sea eficiente y eficaz, en los planos intergubernamental, multilateral y multipartito,

1. *Pedimos* a los parlamentos, Gobiernos y todas las demás partes interesadas que cooperen para desarrollar marcos políticos, reglamentarios y legislativos destinados a mejorar la ciberseguridad y combatir la ciberdelincuencia, y *recomendamos* que ese tipo de marcos:

a) Se desarrollen de una manera abierta y transparente, con la participación de todos los actores gubernamentales y no gubernamentales pertinentes desde el principio;
b) Integren un enfoque de seguridad centrado en las personas e incorporen los principios de estado de derecho, control judicial, proporcionalidad, rendición de cuentas y transparencia;
c) Proporcionen la suficiente financiación para garantizar que las autoridades encargadas de la aplicación de esos marcos están debidamente preparadas –con recursos financieros, técnicos y humanos– para desempeñar su labor;
d) Definan claramente las funciones y responsabilidades de los agentes públicos y privados relevantes de manera que permitan una colaboración significativa y efectiva para conseguir un ciberespacio más seguro;
e) Se basen en las normas técnicas acordadas internacionalmente en materia de ciberseguridad;
f) Sean coherentes con la legislación vigente que se ha desarrollado para el mundo analógico, por ejemplo, la legislación para combatir el discurso de odio o el fraude;

2. *Pedimos asimismo* a los parlamentos que garanticen el debido equilibrio entre las medidas destinadas a mejorar la ciberseguridad y combatir la ciberdelincuencia, por un lado, y la protección de

los derechos humanos y las libertades fundamentales reconocidos internacionalmente por otro, y en particular que:

a) Velen por que los marcos en materia de ciberseguridad se complementen con leyes rigurosas de protección de datos;
b) Alienten a una cooperación eficaz entre los servicios de inteligencia y otros departamentos gubernamentales, y pidan transparencia y rendición de cuentas a los servicios de inteligencia encargados de la ciberseguridad;
c) Eviten el uso de medidas de ciberseguridad con fines políticos, por ejemplo, para dirigirse a políticos de la oposición;

3. *Pedimos además* a los parlamentos que:

a) Entablen un diálogo habitual con los ministerios y las agencias pertinentes, garanticen que el Gobierno presta la atención adecuada a abordar las ciberamenazas, y exijan cuentas a las autoridades de los progresos logrados relativos a la mejora de la ciberseguridad y el combate de la ciberdelincuencia;
b) Consideren los mecanismos institucionales más adecuados para abordar cuestiones relacionadas con las ciberamenazas en los parlamentos, entre otras cuestiones con la aclaración del mandato de las comisiones parlamentarias existentes o la creación de comisiones especiales;
c) Alienten a una cooperación eficaz entre las autoridades públicas y el sector privado para fortalecer la ciberseguridad y generar un entorno de confianza que conduzca a esa cooperación;
d) Examinen las posibilidades del empleo de las tecnologías digitales, como la inteligencia artificial, para luchar contra la ciberdelincuencia, y las debidas salvaguardias de los derechos humanos necesarias para evitar el uso indebido de ese tipo de tecnologías;

4. *Pedimos* a los parlamentarios que:

a) Contribuyan a las iniciativas destinadas a sensibilizar, crear capacidad y desarrollar una cultura de ciberseguridad en toda la sociedad;
b) Traduzcan las cuestiones de ciberseguridad en conceptos accesibles para las personas, ayuden al público a entender lo que está en juego y aumenten la voluntad política para abordar las ciberamenazas;
c) Aprovechen cualquier ocasión de alentar a los integrantes del público a que pongan en práctica una buena ciberhigiene;
d) Centren la atención en fomentar que las mujeres hagan carrera en el ámbito de la ciberseguridad, así como en combatir los incidentes de ciberdelincuencia que tienen como objetivo a las mujeres;
e) Encuentren maneras de llevar la conversación sobre las ciberamenazas al debate político predominante, acaparar la atención de los medios de comunicación y aumentar la presión para que los Gobiernos actúen;
f) Consideren la organización de eventos especiales en los parlamentos para señalar la atención de las ciberamenazas, como “jornadas sobre ciberseguridad” específicas o un espacio dedicado a formular preguntas a los ministerios y las agencias competentes;

5. *Alentamos* a los parlamentos, a tenor del potencial de los instrumentos regionales e internacionales para promover la armonización de los marcos reglamentarios y legislativos en materia de ciberseguridad y ciberdelincuencia y para promover la cooperación internacional, a que:

a) Consideren la ratificación de los instrumentos internacionales vigentes como el Convenio sobre la Ciberdelincuencia (Convenio Budapest) del Consejo de Europa y de instrumentos regionales como la Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales (Convención de Malabo);
b) Se aseguren de que los convenios ratificados se reflejan en las políticas, los reglamentos y las legislaciones nacionales, y se aplican debidamente a nivel nacional;
c) Alienten a sus Gobiernos a que participen en la negociación de nuevos instrumentos sobre ciberdelincuencia al nivel de las Naciones Unidas, así como en los procesos internacionales de elaboración de normas para un comportamiento responsable de los Estados en el ciberespacio;
d) Alienten asimismo a sus Gobiernos a que velen por que sus posiciones en ese tipo de procesos se sustenten en el diálogo con múltiples interesados y que cualquier instrumento nuevo se complemente con las normas vigentes sobre el estado de derecho y los instrumentos existentes en materia de derechos humanos;

6. *Pedimos* a los asociados internacionales para el desarrollo que:

a) Impliquen a los parlamentos en todas las etapas de las iniciativas dedicadas a apoyar el desarrollo de marcos políticos, normativos y legislativos para mejorar la ciberseguridad y combatir la ciberdelincuencia;
b) Desarrollen la capacidad de los parlamentarios de trabajar en cuestiones relacionadas con la ciberseguridad y la ciberdelincuencia, así como en temas de política digital más amplios, por medio de formación y la mejora de las competencias, entre otra cuestiones;

7. *Invitamos* a los parlamentos a que refuercen el diálogo y los intercambios de experiencias con otros parlamentos y órganos parlamentarios, incluido el intercambio de información acerca de iniciativas legislativas nuevas y existentes relacionadas con la ciberseguridad y la ciberdelincuencia en los planos nacional y regional;

8. *Pedimos* a los parlamentos y los parlamentarios que:

a) Contribuyan al fortalecimiento del diálogo nacional entre las diversas partes interesadas sobre cuestiones de política relativas a Internet;
b) Continúen y refuercen su participación en el IGF, intervengan en las iniciativas nacionales y regionales del IGF y consideren la labor llevada a cabo en estos foros como recursos para configurar sus discusiones y actividades parlamentarias;
c) Participen en los procesos mundiales destinados a fortalecer la cooperación digital, como el desarrollo del Pacto Digital Mundial propuesto por el Secretario General de las Naciones Unidas;

9. *Reconocemos* con aprecio la publicación de la Secretaría del IGF de una *guía para cuestiones fundamentales de política digital y las organizaciones y los procesos conexos: herramienta para parlamentarios* (en inglés), y

a) Alentamos a los parlamentarios a que hagan uso de esta herramienta para conformar, según corresponda, su labor en cuestiones de política digital;
b) Alentamos igualmente al mantenimiento de la herramienta como documento vivo y en constante evolución;

10. *Pedimos* al IGF que siga institucionalizando el itinerario parlamentario y que facilite los intercambios habituales entre los parlamentarios y otras partes interesadas del IGF.