Naciones Unidas A/79/214*

Asamblea General

Distr. general
22 de julio de 2024
Español
Original: inglés

Septuagésimo noveno período de sesiones
Tema 93 del programa provisional**
Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional

Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional

Nota del Secretario General

El Secretario General tiene el honor de transmitir a los miembros de la Asamblea General el tercer informe anual sobre los progresos realizados por el grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025).

* Publicado nuevamente por razones técnicas el 2 de octubre de 2024.
** A/79/150.

24-13414* (S) 021024 021024

Se ruega reciclar

Informe del grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025)

I. Introducción

1. En su resolución 75/240, la Asamblea General decidió establecer, a partir de 2021, con miras a asegurar el carácter ininterrumpido y continuo del proceso democrático, inclusivo y transparente de negociación sobre la seguridad en la utilización de las tecnologías de la información y las comunicaciones, bajo los auspicios de las Naciones Unidas, un nuevo grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025), que actuaría por consenso, para seguir elaborando con carácter prioritario las reglas, normas y principios de comportamiento responsable de los Estados, así como las modalidades de aplicación correspondientes y, de ser necesario, introducir cambios o elaborar reglas de comportamiento adicionales; examinar las iniciativas de los Estados encaminadas a garantizar la seguridad en la utilización de las tecnologías de la información y las comunicaciones; entablar, bajo los auspicios de las Naciones Unidas, un diálogo institucional periódico con amplia participación de los Estados; seguir estudiando, con miras a promover el entendimiento común, las amenazas actuales y potenciales en la esfera de la seguridad de la información, incluida la seguridad de los datos, y las posibles medidas de cooperación para prevenir y contrarrestar esas amenazas, y la forma en que el derecho internacional se aplicaba a la utilización de las tecnologías de la información y las comunicaciones por los Estados, así como las medidas de fomento de la confianza y la creación de capacidad; y presentarle en su octogésimo período de sesiones, para su aprobación por consenso, informes anuales sobre los progresos realizados y un informe final sobre los resultados de su labor.

2. El primer informe anual sobre los progresos realizados por el grupo de trabajo, relativo a su período de sesiones de organización y a sus períodos de sesiones sustantivos primero, segundo y tercero, se publicó como documento A/77/275. El segundo informe anual sobre los progresos realizados por el grupo de trabajo, relativo a sus períodos de sesiones sustantivos cuarto y quinto, se publicó como documento A/78/265.

II. Cuestiones de organización

A. Apertura y duración de los períodos de sesiones sustantivos sexto, séptimo y octavo

3. El grupo de trabajo celebró su sexto período de sesiones sustantivo del 11 al 15 de diciembre de 2023, su séptimo período de sesiones sustantivo del 4 al 8 de marzo de 2024 y su octavo período de sesiones sustantivo del 8 al 12 de julio de 2024 en la Sede de las Naciones Unidas.

4. La Oficina de Asuntos de Desarme y el Instituto de las Naciones Unidas de Investigación sobre el Desarme prestaron apoyo sustantivo al grupo de trabajo. El Departamento de la Asamblea General y de Gestión de Conferencias prestó servicios de secretaría.

B. Participantes

5. Los participantes en los períodos de sesiones sustantivos sexto, séptimo y octavo figuran en los documentos A/AC.292/2023/INF/7, A/AC.292/2024/INF/2 y A/AC.292/2024/INF/4, respectivamente.

C. Mesa

6. En sus períodos de sesiones sustantivos sexto, séptimo y octavo, el grupo de trabajo estuvo presidido por el Sr. Burhan Gafoor (Singapur).

D. Organización de los trabajos

7. En la primera sesión del sexto período de sesiones sustantivo, celebrada el 11 de diciembre de 2023, el grupo de trabajo acordó la organización de sus trabajos que figuraba en el documento A/AC.292/2023/4. También aprobó la participación en el grupo de trabajo de las entidades no gubernamentales enumeradas en la lista que figuraba en el documento A/AC.292/2023/INF/6.

8. En la primera sesión del séptimo período de sesiones sustantivo, celebrada el 4 de marzo de 2024, el grupo de trabajo acordó la organización de sus trabajos que figuraba en el documento A/AC.292/2024/1. También aprobó la participación en el grupo de trabajo de las entidades no gubernamentales enumeradas en la lista que figuraba en el documento A/AC.292/2024/INF/1.

9. En la primera sesión del octavo período de sesiones sustantivo, celebrada el 8 de julio de 2024, el grupo de trabajo acordó la organización de sus trabajos que figuraba en el documento A/AC.292/2024/4. También aprobó la participación en el grupo de trabajo de las entidades no gubernamentales enumeradas en la lista que figuraba en el documento A/AC.292/2024/INF/3.

E. Documentación

10. La lista completa de todos los documentos oficiales, documentos de trabajo, documentos técnicos y demás documentación de que dispuso el grupo de trabajo puede consultarse en el sitio web correspondiente (https://meetings.unoda.org/open-ended-working-group-on-information-and-communication-technologies-2021).

F. Labor del grupo de trabajo

11. En su sexto período de sesiones sustantivo, el grupo de trabajo examinó los temas 3, 5 y 6 del programa en sus diez sesiones plenarias.

12. En su séptimo período de sesiones sustantivo, el grupo de trabajo examinó los temas 3, 5 y 6 del programa en sus diez sesiones plenarias.

13. En su octavo período de sesiones sustantivo, el grupo de trabajo examinó los temas del programa 3, 5, 6 y 7 en sus nueve sesiones plenarias.

14. Del 13 al 17 de mayo y el 1 de julio de 2024, la Presidencia celebró reuniones específicas entre períodos de sesiones para escuchar las opiniones sobre los temas sometidos al examen del grupo de trabajo, los cuales figuraban en el mandato del grupo de trabajo establecido en la resolución 75/240 de la Asamblea General y en el programa del grupo de trabajo (A/AC.292/2021/1), de conformidad con las decisiones

de la Asamblea 77/512 y 78/541. En dichas reuniones, presentaron exposiciones informativas especializadas sobre temas seleccionados expertos escogidos de una lista de expertos designados presentada por las delegaciones y participaron las partes interesadas.

15. El 9 de mayo de 2024, la Presidencia convocó la primera reunión de puntos de contacto del directorio mundial de puntos de contacto, de conformidad con lo dispuesto en el documento A/78/265 y en la decisión 78/541 de la Asamblea General. La primera reunión de puntos de contacto también marcó la puesta en marcha oficial del directorio.

16. El 10 de mayo de 2024, la Presidencia convocó la primera mesa redonda mundial de alto nivel sobre la creación de capacidad en materia de seguridad de la tecnología de la información y las comunicaciones, de conformidad con lo dispuesto en la decisión 78/541 de la Asamblea General, a fin de proporcionar una plataforma para los profesionales de la creación de capacidad, los representantes de los Estados y las partes interesadas para intercambiar ideas, compartir buenas prácticas y forjar alianzas con el objetivo de mejorar las sinergias y avanzar en la labor de la comunidad internacional relacionada con la creación de capacidad de formas concretas.

17. El 28 de septiembre de 2023 y el 31 de enero, el 27 de marzo y el 10 de junio de 2024, la Presidencia convocó reuniones oficiosas virtuales para informar a las delegaciones sobre los elementos que estaba estudiando el grupo de trabajo.

18. El 13 de diciembre de 2023 y el 6 de marzo y el 10 de julio de 2024, de conformidad con las modalidades acordadas para la participación de las partes interesadas, se celebraron sesiones dedicadas a las partes interesadas durante la sexta sesión del sexto período de sesiones sustantivo, la sexta sesión del séptimo período de sesiones sustantivo y la quinta sesión del octavo período de sesiones sustantivo.

19. Los días 6 de diciembre de 2023 y 28 de febrero y 3 de julio de 2024, la Presidencia celebró debates consultivos oficiosos con las partes interesadas, entre ellas empresas, organizaciones no gubernamentales y círculos académicos, para escuchar sus opiniones sobre los temas sometidos al examen del grupo de trabajo de composición abierta, los cuales figuraban en el mandato del grupo de trabajo establecido en la resolución 75/240 de la Asamblea General y en el programa del grupo de trabajo (A/AC.292/2021/1), e ideas concretas que el grupo de trabajo podría considerar en el futuro.

III. Aprobación del informe

20. En su octavo período de sesiones sustantivo, el 12 de julio de 2024, el grupo de trabajo examinó el tema 7 del programa, titulado “Aprobación de los informes anuales sobre los progresos realizados”, y aprobó el proyecto de informe del grupo de trabajo de composición abierta (A/AC.292/2024/L.1). También decidió incluir en su informe el resultado de los debates del grupo de trabajo sobre el tema 5 del programa, que figuraba en el documento A/AC.292/2024/CRP.1 (véase el anexo).

21. Las declaraciones en explicación de posición se recogerán en un compendio que se publicará como documento A/AC.292/2024/INF/5.

Anexo*

Informe sobre los progresos realizados en los debates del grupo de trabajo sobre el tema 5 del programa

A. Sinopsis

1. Los períodos de sesiones oficiales sexto, séptimo y octavo y las reuniones específicas entre períodos de sesiones del grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025) se celebraron en un entorno geopolítico que seguía siendo difícil, en el que iba en aumento la preocupación por el uso malintencionado, por parte de agentes estatales y no estatales, de las tecnologías de la información y las comunicaciones (TIC), el cual repercutía en la paz y la seguridad internacionales.

2. En esos períodos de sesiones, los Estados recordaron las decisiones y resoluciones consensuadas de la Asamblea General en las que los Estados acordaron que debían guiarse en su uso de las TIC por los informes del grupo de trabajo y del Grupo de Expertos Gubernamentales[1]. A ese respecto, los Estados recordaron además las contribuciones del primer grupo de trabajo de composición abierta, establecido en virtud de la resolución 73/27 de la Asamblea General, que concluyó su labor en 2021 mediante su informe final acordado por consenso[2], y tomaron nota del resumen de la Presidencia y de la lista de propuestas no exhaustivas anexa al resumen de la Presidencia, y recordaron las contribuciones del sexto Grupo de Expertos Gubernamentales, establecido en virtud de la Resolución 73/266 de la Asamblea General, que concluyó su labor en 2021 mediante su informe final acordado por consenso[3].

3. Además, los Estados reafirmaron los informes anuales de consenso primero y segundo sobre los progresos realizados por el actual grupo de trabajo[4], el informe de consenso del grupo de trabajo de 2021 sobre los avances en la esfera de las TIC en el contexto de la seguridad internacional y los informes de consenso de los Grupos de Expertos Gubernamentales de 2010, 2013, 2015 y 2021[5]. Los Estados recordaron y reafirmaron que, en esos informes, los Grupos "recomendaron 11 normas voluntarias y no vinculantes de comportamiento responsable de los Estados y reconocieron que con el tiempo podrían elaborarse más normas", y "recomendaron medidas específicas de fomento de la confianza, desarrollo de la capacidad y cooperación". Los Estados también recordaron y reafirmaron que "el derecho internacional, en particular la Carta de las Naciones Unidas, e[ra] aplicable y esencial para mantener la paz, la seguridad y la estabilidad en el entorno de las TIC"[6]. Esos elementos consolidaban un marco acumulativo y evolutivo[7] de comportamiento responsable de los Estados en el uso de las TIC que proporcionaba una base sobre la que el actual grupo de trabajo y el futuro mecanismo permanente construían su labor.

4. El grupo de trabajo recordó su mandato, que figuraba en la resolución 75/240 de la Asamblea General, como sigue: "[a]ctuará por consenso para seguir elaborando

---

* Publicado sin revisión editorial.

[1] Decisiones 77/512 y 75/564 y resoluciones 70/237 y 76/19 de la Asamblea General.

[2] A/75/816.

[3] A/76/135.

[4] A/77/275 y A/78/265, respectivamente.

[5] A/65/201, A/68/98, A/70/174 y A/76/135.

[6] Informe del grupo de trabajo de 2021 (A/75/816), anexo I, párr. 7.

[7] Informe del Grupo de Expertos Gubernamentales de 2021 (A/76/135), párr. 2, y resolución 76/19 de la Asamblea General, aprobada por consenso.

con carácter prioritario las reglas, normas y principios de comportamiento responsable de los Estados, así como las modalidades de aplicación correspondientes y, de ser necesario, introducir cambios o elaborar reglas de comportamiento adicionales; examinar las iniciativas de los Estados encaminadas a garantizar la seguridad en la utilización de las tecnologías de la información y las comunicaciones; entablar, bajo los auspicios de las Naciones Unidas, un diálogo institucional periódico con amplia participación de los Estados; seguir estudiando, con miras a promover el entendimiento común, las amenazas actuales y potenciales en la esfera de la seguridad de la información, incluida la seguridad de los datos, y las posibles medidas de cooperación para prevenir y contrarrestar esas amenazas, y la forma en que el derecho internacional se aplica a la utilización de las tecnologías de la información y las comunicaciones por los Estados, así como las medidas de fomento de la confianza y la creación de capacidad; y presentarle en su octogésimo período de sesiones, para su aprobación por consenso, informes anuales sobre los progresos realizados y un informe final sobre los resultados de su labor". A ese respecto, el grupo de trabajo reconoció la importancia de abordar su mandato de forma equilibrada y la necesidad de prestar la debida atención tanto a seguir desarrollando entendimientos comunes entre los Estados sobre la seguridad en el uso de las TIC como a impulsar la aplicación de los compromisos existentes.

5. A medida que el grupo de trabajo profundizaba en sus deliberaciones, aumentaba entre los Estados el reconocimiento de las interconexiones entre todas las cuestiones de las que se ocupaba. A ese respecto, los Estados pusieron de relieve que la labor del grupo de trabajo y del futuro mecanismo permanente revestiría un carácter integrado, transversal y orientado a las políticas.

6. El grupo de trabajo reconoció que la creación de capacidad era una importante medida de fomento de la confianza y un tema transversal a todos los pilares de la labor del grupo de trabajo y que era esencial disponer de un enfoque integral de la creación de capacidad en el contexto de la seguridad de las TIC. A ese respecto, era indispensable encontrar soluciones sostenibles, eficaces y asequibles.

7. El grupo de trabajo también puso de relieve que crear capacidad era fundamental para desarrollar los recursos, las competencias, las políticas y las instituciones necesarias a fin de fomentar la resiliencia y la seguridad de las TIC de los Estados y para acelerar la transformación digital de los Estados y la implementación de la Agenda 2030 para el Desarrollo Sostenible. Los Estados reconocieron que crear capacidad favorecía el marco de comportamiento responsable de los Estados en el uso de las TIC y contribuía a construir un entorno de las TIC abierto, seguro, estable, accesible, pacífico e interoperable. Dada la rapidez con la que evolucionaba el panorama digital, era preciso acelerar los esfuerzos de creación de capacidad adaptados a las necesidades, por ser una de las funciones clave del futuro mecanismo permanente, dirigida a colmar las brechas digitales y a procurar que todos los Estados pudieran sacar partido de las tecnologías digitales de forma segura. En ese sentido, los Estados reafirmaron los principios de creación de capacidad sobre la seguridad de las TIC aprobados en el informe del grupo de trabajo de 2021 y contenidos en el segundo informe anual sobre los progresos realizados.

8. El grupo de trabajo tiene la determinación de implicar a las partes interesadas de manera sistemática, sostenida y sustantiva, de acuerdo con las modalidades acordadas por el procedimiento de acuerdo tácito el 22 de abril de 2022 y adoptadas formalmente en la primera reunión del tercer período de sesiones del grupo de trabajo el 25 de julio de 2022, y en línea con su mandato, contenido en la resolución 75/240 de la Asamblea General, en el sentido de interactuar, según proceda, con otras partes

interesadas, entre ellas empresas, organizaciones no gubernamentales y círculos académicos[8].

9. El grupo de trabajo reconoció que las organizaciones regionales y subregionales podían seguir desempeñando un papel importante en la aplicación del marco de comportamiento responsable de los Estados en el uso de las TIC. Además, los intercambios regionales, interregionales e interinstitucionales podían establecer nuevas vías de colaboración, cooperación y aprendizaje mutuo. Dado que no todos los Estados eran miembros de una organización regional y no todas las organizaciones regionales se centraban en la cuestión de la seguridad en el uso de las TIC, el grupo de trabajo señaló que los esfuerzos regionales eran complementarios a su labor[9].

10. El grupo de trabajo acogió con agrado la gran participación de delegadas en sus períodos de sesiones y la prominencia de una perspectiva de género en sus discusiones. El grupo de trabajo subrayó la importancia de reducir la brecha digital de género y promover la participación plena, igualitaria y significativa y el liderazgo de las mujeres en los procesos de toma de decisiones vinculados a la utilización de las TIC en el contexto de la seguridad internacional.

11. Este tercer informe anual sobre los progresos realizados incluye acciones concretas y medidas de cooperación para hacer frente a las amenazas relacionadas con las TIC y promover un entorno de TIC abierto, seguro, estable, accesible y pacífico y, en ese sentido, se basa en los informes anuales sobre los progresos realizados primero y segundo, aprobados por consenso en las decisiones de la Asamblea General 77/512 y 78/541, respectivamente. Reconociendo que el grupo de trabajo se encuentra inmerso en las deliberaciones en curso y proseguirá sus debates sustantivos hasta la finalización de su mandato en 2025, este tercer informe anual sobre los progresos realizados no pretende ser un resumen exhaustivo de los debates de los Estados, sino que tiene por objeto recoger los avances concretos alcanzados por el grupo de trabajo hasta la fecha, basándose también en la hoja de ruta para los debates que figura en los informes anuales sobre los progresos realizados primero y segundo. El tercer informe anual sobre los progresos realizados se presentará a la Asamblea General de acuerdo con el mandato del grupo de trabajo, recogido en la resolución 75/240.

B. Amenazas actuales y potenciales

12. Durante los períodos de sesiones sexto, séptimo y octavo y las reuniones específicas entre períodos de sesiones del grupo de trabajo, los Estados continuaron debatiendo sobre las amenazas actuales y potenciales. A ese respecto, los Estados recordaron el alcance de la labor del grupo de trabajo para considerar las amenazas relacionadas con las TIC en el contexto de la seguridad internacional y emprendieron debates sobre las amenazas actuales y potenciales relacionadas con las TIC a través de ese prisma específico. Los Estados, recordando las amenazas señaladas en los informes anuales sobre los progresos realizados primero y segundo, en el informe del grupo de trabajo de 2021 y en los informes del Grupo de Expertos Gubernamentales, reiteraron la creciente preocupación por el hecho de que las amenazas en el uso de las TIC en el contexto de la seguridad internacional se habían intensificado y habían evolucionado de forma significativa en el entorno geopolítico imperante, que seguía siendo problemático.

[8] Primer informe anual sobre los progresos realizados, párr. 4, y segundo informe anual sobre los progresos realizados, párr. 6.

[9] Primer informe anual sobre los progresos realizados, párr. 5, y segundo informe anual sobre los progresos realizados, párr. 7.

13. Los Estados recordaron que varios Estados estaban desarrollando capacidades de TIC con fines militares. También recordaron que el uso de las TIC en futuros conflictos entre Estados era cada vez más probable y señalaron que las TIC ya se habían utilizado en conflictos en diferentes regiones. El aumento continuo de los incidentes de uso malintencionado de las TIC por agentes estatales y no estatales, incluidos terroristas y grupos delictivos, era una tendencia perturbadora. Algunos agentes no estatales habían demostrado tener capacidades de TIC que antes solo estaban al alcance de los Estados[10].

14. Los Estados expresaron preocupación por el aumento de las actividades malintencionadas relacionadas con las TIC que afectaban a las infraestructuras críticas y las infraestructuras críticas de información, como las de los sectores de la salud, la navegación marítima, la aviación, las finanzas y la energía. Esas infraestructuras críticas e infraestructuras críticas de información podían servir para prestar servicios esenciales a través de las fronteras y las jurisdicciones, y los ataques informáticos contra ellas podían dar lugar a una concatenación de efectos en los planos nacional, regional y mundial[11]. Los Estados resaltaron que determinar qué infraestructuras designar como críticas era prerrogativa de cada Estado[12].

15. Los Estados recalcaron que las actividades malintencionadas relacionadas con las TIC que afectaban a las infraestructuras críticas y las infraestructuras críticas de información que menoscababan la confianza entre los Estados y en los procesos políticos y electorales y las instituciones públicas o que afectaban a la disponibilidad general o la integridad de Internet también eran un problema real y creciente[13].

16. Los Estados pusieron de relieve la necesidad de proteger los cables submarinos y las redes de comunicación orbitales frente a actividades malintencionadas que podrían causar daños o interrupciones importantes en las telecomunicaciones y afectar a la infraestructura técnica esencial para la disponibilidad y la integridad de Internet en amplias zonas del planeta.

17. Los Estados expresaron preocupación por las actividades malintencionadas relacionadas con las TIC dirigidas a organizaciones internacionales y organizaciones humanitarias, que podrían perturbar la capacidad de dichas organizaciones de cumplir sus respectivos mandatos con seguridad e independencia y socavar la confianza en su labor.

18. Los Estados observaron un aumento preocupante del uso malintencionado por los Estados de campañas de información encubiertas con ayuda de las TIC para influir en los procesos, los sistemas y la estabilidad general de otros Estados. Estos usos socavaban la confianza y podían dar lugar a escaladas y amenazar la paz y la seguridad internacionales. También podían suponer un daño directo o indirecto para las personas[14]. Los Estados expresaron especial preocupación por las actividades malintencionadas relacionadas con las TIC destinadas a interferir en los asuntos internos de los Estados[15].

19. Los Estados expresaron preocupación por la explotación de las vulnerabilidades de los productos de las TIC y el uso de funciones ocultas dañinas, en particular cuando estas cuestiones afectaban a la paz y la seguridad internacionales. Los Estados

[10] Informe del grupo de trabajo de 2021 (A/75/816), anexo I, párr. 16; segundo informe anual sobre los progresos realizados, párr. 11.
[11] Segundo informe anual sobre los progresos realizados, párr. 12.
[12] Informe del grupo de trabajo de 2021 (A/75/816), párr. 18.
[13] Informe del grupo de trabajo de 2021 (A/75/816), anexo I, párr. 18; segundo informe anual sobre los progresos realizados, párr. 13.
[14] Segundo informe anual sobre los progresos realizados, párr. 14.
[15] Segundo informe anual sobre los progresos realizados, párr. 13.

también señalaron la importante amenaza informática que ello representaba para la integridad de las cadenas de suministro[16].

20. Los Estados destacaron la preocupación por el uso de programas maliciosos, como los programas secuestradores, troyanos y programas maliciosos borradores, y técnicas como la suplantación de identidad, la intercepción y la denegación de servicio distribuida. Se expresó especial preocupación porque cada vez más agentes malintencionados cometían, en diferentes regiones del mundo, ataques con programas secuestradores, facilitados en parte por la posibilidad de contratar ese tipo de ataques como servicio. Los Estados subrayaron con preocupación que la creciente frecuencia, escala y gravedad de los ataques con programas secuestradores causaba daños, interrumpía servicios esenciales para la población y podía repercutir en la paz y la seguridad internacionales. Los Estados señalaron la necesidad de encarar de manera integral todos los elementos de la amenaza que planteaban los programas secuestradores, por medios como perseguir a quienes los utilizaban, luchar contra los programas maliciosos que usaban y contra su difusión y combatir la financiación ilícita de sus actividades. Los Estados también resaltaron con preocupación el aumento del robo de criptomonedas y su utilización para financiar actividades malintencionadas relacionadas con las TIC, lo cual podría afectar a la seguridad internacional.

21. Los Estados señalaron el crecimiento del mercado de capacidades de intrusión informática de libre contratación, así como la mayor vulnerabilidad del equipo y los programas informáticos, en particular en la web oscura. Los Estados expresaron preocupación porque la facilidad con la que los agentes estatales y no estatales podían adquirir esas capacidades las hacía más susceptibles a ser utilizadas de modo ilegítimo y malintencionado y podía dificultar la tarea de mitigar las amenazas que planteaban y defenderse de ellas, y subrayaron que dichas capacidades podían utilizarse de manera compatible con el derecho internacional. Los Estados expresaron preocupación también porque la difusión de las capacidades informáticas de intrusión por agentes estatales y no estatales podría contribuir a una escalada no intencionada y amenazar la paz y la seguridad internacionales.

22. Los Estados señalaron que, en sí mismas, las tecnologías eran neutras y que las tecnologías nuevas y emergentes, como la inteligencia artificial y la informática cuántica, estaban ampliando las oportunidades de desarrollo. Al mismo tiempo, sus propiedades y características, en constante evolución, podían llegar a repercutir en el uso de las TIC en el contexto de la seguridad internacional creando nuevos vectores y vulnerabilidades en la esfera de las TIC. Esas tecnologías también podían impulsar la velocidad y el potencial de ataque de las actividades malintencionadas relacionadas con las TIC[17]. La confluencia de las nuevas tecnologías también podría agravar los riesgos.

23. Los Estados expresaron especial preocupación por la seguridad y la protección de los sistemas de inteligencia artificial, así como por los datos utilizados para entrenar modelos de aprendizaje automático e inteligencia artificial en el contexto de la seguridad de las TIC. La inteligencia artificial podía emplearse para mejorar la seguridad de las TIC, fomentar la resiliencia, mejorar el tiempo de respuesta a los incidentes informáticos y reforzar las redes. Los Estados pusieron de relieve la probabilidad de que la inteligencia artificial incrementara el volumen y el impacto de los ataques informáticos al desarrollar y perfeccionar las tácticas, técnicas y procedimientos existentes. Esas operaciones podrían aumentar el riesgo de generar

[16] Segundo informe anual sobre los progresos realizados, párr. 15.

[17] Primer informe anual sobre los progresos realizados por el grupo de trabajo (A/77/275), párr. 11; informe del Grupo de Expertos Gubernamentales de 2021 (A/76/135), párr. 11, y resolución 76/19 de la Asamblea General, aprobada por consenso.

efectos concatenados que podrían causar daños no deseados, incluso a las personas y a las infraestructuras críticas. Los Estados recalcaron que era necesario comprender mejor los riesgos asociados a las tecnologías nuevas y emergentes, en particular la inteligencia artificial, respecto de su relación con la seguridad de las TIC, y aplicar y reforzar medidas de seguridad durante todo el ciclo de vida de esas tecnologías a fin de aprovechar plenamente las oportunidades que ofrecían. Los Estados destacaron que redundaba en interés de todos los Estados promover la utilización de las tecnologías nuevas y emergentes con fines pacíficos.

24. Teniendo en cuenta el crecimiento y la agregación de datos asociados a las tecnologías nuevas y emergentes, los Estados también señalaron la creciente importancia de la protección y la seguridad de los datos[18].

25. Los Estados observaron con preocupación que garantizar que no se explotaran con fines maliciosos las vulnerabilidades de la tecnología operativa y de los dispositivos, plataformas, máquinas u objetos informáticos interconectados que constituyen la Internet de los objetos se había convertido en un importante desafío.

26. Los Estados siguieron llamando la atención sobre la necesidad de una perspectiva de género a la hora de abordar las amenazas relacionadas con las TIC y sobre los riesgos específicos a los que se enfrentaban las personas en situaciones de vulnerabilidad. Los Estados siguieron insistiendo en que los beneficios de la tecnología digital no eran disfrutados por todos por igual y, en consecuencia, subrayaron la necesidad de prestar la debida atención a la creciente brecha digital en el contexto de la aceleración de la implementación de la Agenda 2030 para el Desarrollo Sostenible, respetando al mismo tiempo las necesidades y prioridades nacionales de los Estados[19].

27. Los Estados recordaron que cualquier uso de las TIC por los Estados de forma incompatible con las obligaciones que contrajeron en el marco de comportamiento responsable de los Estados en el uso de las TIC, que incluye normas voluntarias, el derecho internacional y medidas de fomento de la confianza, menoscababa la paz y la seguridad internacionales, la confianza y la estabilidad entre los Estados[20].

28. Los Estados continuaron expresando preocupación por el hecho de que la falta de concienciación sobre las amenazas actuales y potenciales y la falta de capacidades adecuadas para detectar las actividades malintencionadas relacionadas con las TIC, defenderse de ellas o darles respuesta pudieran hacerlos más vulnerables[21]. A la luz de la evolución del panorama de las amenazas en el uso de las TIC en el contexto de la seguridad internacional, y reconociendo que ningún Estado estaba al abrigo de estas amenazas, los Estados subrayaron la urgencia de aumentar la concienciación y profundizar en la comprensión de esas amenazas y de implantar y seguir desarrollando medidas de cooperación[22] e iniciativas de creación de capacidad en el marco acumulativo y evolutivo de comportamiento responsable de los Estados[23].

[18] Segundo informe anual sobre los progresos realizados, párr. 17.
[19] Segundo informe anual sobre los progresos realizados, párr. 18.
[20] Segundo informe anual sobre los progresos realizados, párr. 19.
[21] Informe del grupo de trabajo de 2021 (A/75/816), anexo I, párr. 20.
[22] Informe del grupo de trabajo de 2021 (A/75/816), anexo I, párr. 22.
[23] Segundo informe anual sobre los progresos realizados, párr. 20.

Próximas medidas recomendadas

29. **Se recomienda a los Estados que sigan intercambiando en el grupo de trabajo puntos de vista sobre las amenazas actuales y potenciales para la seguridad en el uso de las TIC en el contexto de la seguridad internacional, teniendo en cuenta los párrafos 12 a 28 del presente anexo, y que prosigan los debates centrados en posibles medidas de cooperación para hacer frente a esas amenazas, reconociendo, a ese respecto, que la adhesión de todos los Estados al marco de comportamiento responsable de los Estados en el uso de las TIC sigue siendo fundamental para hacer frente a las amenazas actuales y potenciales para la seguridad internacional relacionadas con las TIC, y reafirmando que es vital que el marco se respete y aplique para cumplir ese objetivo.**

30. **Se invita a los Estados a que presenten documentos de trabajo sobre posibles formas de concienciar de las amenazas existentes y potenciales y de profundizar en su comprensión, y a que determinen posibles medidas de cooperación e iniciativas de creación de capacidad para que los Estados puedan detectar esas amenazas, defenderse de ellas o darles respuesta. Se solicita a la Secretaría de las Naciones Unidas que publique esos documentos en el sitio web del grupo de trabajo para referencia de todos los Estados y para que el grupo de trabajo pueda seguir examinándolos en sus siguientes períodos de sesiones.**

C. Reglas, normas y principios de comportamiento responsable de los Estados

31. Durante los períodos de sesiones sexto, séptimo y octavo y las reuniones específicas entre períodos de sesiones del grupo de trabajo, los Estados continuaron debatiendo sobre las reglas, normas y principios de comportamiento responsable de los Estados. Reafirmando el marco acumulativo y evolutivo de comportamiento responsable de los Estados en el uso de las TIC, los Estados hicieron propuestas concretas y orientadas a la acción acerca de las reglas, normas y principios. A continuación se presenta una lista no exhaustiva de propuestas con distintos niveles de apoyo por parte de los Estados, que pueden ser desarrolladas y complementadas en los próximos períodos de sesiones del grupo de trabajo:

a) Las normas voluntarias no vinculantes de comportamiento responsable de los Estados podían reducir los riesgos para la paz, la seguridad y la estabilidad internacionales y contribuían notablemente a aumentar la previsibilidad y reducir los riesgos de percepciones erróneas y, de este modo, coadyuvaban a la prevención de los conflictos. Los Estados destacaron que dichas normas reflejaban las expectativas y los estándares de la comunidad internacional en cuanto al comportamiento de los Estados en su utilización de las TIC y permitían a la comunidad internacional evaluar las actividades de los Estados[24];

b) Como se establecía en la norma c)[25], los Estados seguían reconociendo que los Estados no debían permitir a sabiendas que su territorio fuera utilizado para cometer hechos internacionalmente ilícitos utilizando TIC y se mostrarían favorables a celebrar nuevos debates para seguir forjando entendimientos comunes intercambiando experiencias nacionales y regionales;

[24] Informe del grupo de trabajo de 2021 (A/75/816), anexo I, párrs. 64 y 65; segundo informe anual sobre los progresos realizados, párr. 23 b).

[25] Norma c): Los Estados no deben permitir a sabiendas que su territorio sea utilizado para cometer hechos internacionalmente ilícitos utilizando TIC.

c) Como se establecía en las normas f)[26] y g)[27], los Estados subrayaron la importancia de proteger las infraestructuras críticas y las infraestructuras críticas de información. Los Estados destacaron que la actividad en la esfera de las TIC que intencionadamente causaba un perjuicio a las infraestructuras críticas o las infraestructuras críticas de información o dificultaba de otro modo su utilización y funcionamiento para prestar servicios al público podía tener efectos concatenados a nivel nacional, regional y mundial. Suponía un elevado riesgo de daños para la población y podía dar lugar a escaladas[28];

d) En vista de lo anterior, los Estados subrayaron la necesidad de seguir reforzando las medidas para proteger todas las infraestructuras críticas y las infraestructuras críticas de información de las amenazas de las TIC y propusieron aumentar los intercambios sobre las mejores prácticas en materia de protección de esas infraestructuras, incluido el intercambio de políticas nacionales, y de recuperación tras incidentes de TIC que afectaran a las infraestructuras críticas y las infraestructuras críticas de información. Los Estados resaltaron que las medidas de protección específicas para las infraestructuras críticas y las infraestructuras críticas de información podrían abarcar la designación voluntaria de infraestructuras críticas e infraestructuras críticas de información[29], evaluaciones de riesgos exhaustivas, actividades de concienciación y capacitación en TIC y la formulación de los requisitos y directrices reglamentarios nacionales pertinentes. Los Estados resaltaron que determinar qué infraestructuras designar como críticas era prerrogativa de cada Estado.[30] Los Estados hicieron hincapié en la necesidad de cultivar una cultura de mejora continua para adaptarse a la evolución de las amenazas que las TIC podían plantear a las infraestructuras críticas y las infraestructuras críticas de información. Los Estados también reconocieron que la creación de capacidad podía ayudar a los operadores de infraestructuras críticas e infraestructuras críticas de información en ese sentido;

e) Como se establecía en la norma i)[31], los Estados siguieron poniendo de relieve que se podrían reforzar la cooperación y la asistencia para garantizar la integridad de la cadena de suministro y evitar el uso de funciones ocultas perjudiciales. Entre las medidas razonables para promover la apertura y garantizar la integridad, la estabilidad y la seguridad de la cadena de suministro se podían incluir el establecimiento de políticas y programas para promover objetivamente la adopción de buenas prácticas por parte de los proveedores y vendedores de equipos y sistemas de TIC con el fin de fomentar la confianza internacional en la integridad y la seguridad de los productos y servicios de las TIC, mejorar la calidad y promover la elección, así como medidas de cooperación tales como intercambios de buenas prácticas sobre la

[26] Norma f): Un Estado no debe realizar ni apoyar a sabiendas actividades en la esfera de las TIC contrarias a las obligaciones que le incumben en virtud del derecho internacional que dañen intencionadamente infraestructuras fundamentales o dificulten de otro modo la utilización y funcionamiento de infraestructuras fundamentales que prestan servicios al público.

[27] Norma g): Los Estados deben tomar las medidas apropiadas para proteger las infraestructuras fundamentales frente a amenazas relacionadas con las TIC, teniendo en cuenta la resolución 58/199 de la Asamblea General.

[28] Informe del Grupo de Expertos Gubernamentales de 2021 (A/76/135), párr. 42, y resolución 76/19 de la Asamblea General, aprobada por consenso; segundo informe anual sobre los progresos realizados, párr. 23 c).

[29] Los Estados resaltaron que determinar qué infraestructuras designar como críticas era prerrogativa de cada Estado (informe del grupo de trabajo de 2021 (A/75/816), párr. 18).

[30] Informe del grupo de trabajo de 2021 (A/75/816), párr. 18.

[31] Norma i): Los Estados deben adoptar 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 las TIC. Los Estados deben tratar de evitar la proliferación de técnicas e instrumentos malignos en la esfera de las TIC, así como el uso de funciones ocultas perniciosas.

gestión de riesgos en la cadena de suministro; el desarrollo y la aplicación de reglas y normas comunes interoperables a nivel mundial para la seguridad de la cadena de suministro; y otros enfoques destinados a disminuir las vulnerabilidades de la cadena de suministro[32];

f) Los Estados también hicieron hincapié en que la seguridad debía integrarse en el diseño y la fabricación de los productos de las TIC y en que debía favorecerse que los productos incorporaran características de seguridad por encima de que llegaran rápido a los mercados;

g) Los Estados siguieron señalando el papel crucial que desempeñaba el sector privado en la promoción de la apertura y en la garantía de la integridad, estabilidad y seguridad de la cadena de suministro, así como en la prevención de la proliferación de herramientas y técnicas malintencionadas en la esfera de las TIC y del uso de funciones ocultas perjudiciales. Los Estados destacaron que las alianzas público-privadas eran fundamentales para el desarrollo y la promoción de las mejores prácticas a la hora de garantizar la integridad de la cadena de suministro, y alentaron el intercambio de información y de mejores prácticas entre los Estados, así como con la participación de las partes interesadas pertinentes. Los Estados también debían seguir alentando al sector privado a desempeñar un papel adecuado para mejorar la seguridad de las TIC y de su uso, incluida la seguridad de la cadena de suministro de productos de las TIC, de conformidad con las leyes y normativas nacionales de los países en los que operaba[33];

h) Los Estados afirmaron la importancia de apoyar e impulsar los esfuerzos para aplicar las normas que los Estados se habían comprometido a seguir en los planos mundial, regional y nacional[34];

i) Los Estados tomaron nota de la lista voluntaria de medidas prácticas para aplicar las normas voluntarias y no vinculantes sobre el comportamiento responsable de los Estados en el uso de las TIC que figura en el anexo A del presente informe. Los Estados sugirieron que la lista se considerara un documento en evolución que podría seguir debatiéndose y actualizándose en los siguientes períodos de sesiones del grupo de trabajo. Al utilizar la lista deberían tenerse en cuenta las diferencias técnicas entre los Estados, la diversidad de sistemas nacionales y las especificidades regionales. Los Estados expresaron reconocimiento por las orientaciones sobre la aplicación proporcionadas en el informe del Grupo de Expertos Gubernamentales de 2021[35] y señalaron que había otros recursos disponibles que podían ayudar a los Estados a aplicar las reglas, normas y principios existentes. Al mismo tiempo, los Estados reconocieron que la aplicación no se ajustaba a una única solución;

j) Los Estados recordaron el mandato del grupo de trabajo, enunciado en la resolución 75/240 de la Asamblea General, de, entre otras cosas, “seguir elaborando con carácter prioritario las reglas, normas y principios de comportamiento responsable de los Estados, así como las modalidades de aplicación correspondientes y, de ser necesario, introducir cambios o elaborar reglas de comportamiento adicionales”[36];

k) Dadas las características particulares de las TIC, los Estados reafirmaron que podrían seguir desarrollándose nuevas normas. Los Estados también llegaron a la conclusión de que seguir desarrollando normas y aplicar las ya existentes no eran

[32] Segundo informe anual sobre los progresos realizados, párr. 23 d).
[33] Segundo informe anual sobre los progresos realizados, párr. 23 e).
[34] Informe del grupo de trabajo de 2021 (A/75/816), párr. 27.
[35] A/76/135.
[36] Resolución 75/240 de la Asamblea General, párr. 1; segundo informe anual sobre los progresos realizados, párr. 23 a).

actividades mutuamente excluyentes, sino que podían ocurrir simultáneamente[37]. A ese respecto, se hicieron varias propuestas de posibles nuevas normas, las cuales siguen sometidas al examen de los Estados;

l) A ese respecto, los Estados propusieron seguir debatiendo sobre la lista de propuestas no exhaustivas formuladas sobre la elaboración de reglas, normas y principios de comportamiento responsable de los Estados (adjunta al resumen de la Presidencia en el informe del grupo de trabajo de 2021) tras la recomendación recogida en el informe del grupo de trabajo de 2021. Los Estados también propusieron que el actual grupo de trabajo prosiguiera sus deliberaciones sobre la posibilidad de elaborar normas adicionales.

Próximas medidas recomendadas

32. **Se recomienda a los Estados que sigan intercambiando puntos de vista en el grupo de trabajo sobre reglas, normas y principios de comportamiento responsable de los Estados en el uso de las TIC, teniendo en cuenta los párrafos 31 a) a l) del presente anexo, en los próximos períodos de sesiones sustantivos del grupo de trabajo.**

33. **Se recomienda a los Estados que continúen esforzándose por aplicar las normas y que examinen y actualicen la lista voluntaria de medidas prácticas (anexo A), que es un documento en evolución, con vistas a formular una recomendación por consenso sobre la lista a más tardar en julio de 2025.**

34. **Se recomienda a los Estados que prosigan los debates sobre posibles normas adicionales de comportamiento responsable de los Estados en el uso de las TIC durante los próximos períodos de sesiones del grupo de trabajo, sobre la base de los debates mantenidos en los períodos de sesiones anteriores.**

D. Derecho internacional

35. Durante los períodos de sesiones sexto, séptimo y octavo y las reuniones específicas entre períodos de sesiones del grupo de trabajo, reafirmando el marco acumulativo y evolutivo de comportamiento responsable de los Estados en el uso de las TIC, y reafirmando además que el derecho internacional, en particular la Carta de las Naciones Unidas, era aplicable y esencial para mantener la paz, la seguridad y la estabilidad y promover un entorno de TIC abierto, seguro, estable, accesible y pacífico, los Estados continuaron los debates sobre la aplicación del derecho internacional al uso de las TIC. El grupo de trabajo mantuvo debates centrados y en profundidad sobre temas de la lista no exhaustiva de los párrafos 29 a) y b) del segundo informe anual sobre los progresos realizados, así como sobre las propuestas contenidas en el informe del grupo de trabajo de 2021 y en el resumen de la Presidencia, cuando resultó pertinente[38].

36. Al emprender esos debates específicos, los Estados se guiaron por la recomendación del primer informe anual sobre los progresos realizados de que los Estados entablaran debates específicos sobre temas de la lista no exhaustiva que figura en los párrafos siguientes[39]:

a) “El grupo de trabajo podría convocar debates sobre temas específicos relacionados con el derecho internacional. Estos debates deberían centrarse en la identificación de áreas de convergencia y consenso. La lista abierta y no exhaustiva

[37] Informe del grupo de trabajo de 2021 (A/75/816), párr. 29.
[38] Segundo informe anual sobre los progresos realizados, párr. 28.
[39] Segundo informe anual sobre los progresos realizados, párrs. 29 a) y b).

de los temas propuestos por los Estados para continuar el debate en el marco del derecho internacional incluye: de qué forma se aplica el derecho internacional, en particular la Carta de las Naciones Unidas, al uso de las TIC; la soberanía; la igualdad soberana; la no intervención en los asuntos internos de otros Estados; el arreglo pacífico de controversias; la responsabilidad del Estado y la diligencia debida; el respeto de los derechos humanos y las libertades fundamentales; la posibilidad de que existan lagunas en el entendimiento común sobre cómo se aplica el derecho internacional; y las propuestas contenidas en el informe del grupo de trabajo de 2021 y el resumen de la Presidencia, cuando sea pertinente";

b) El grupo de trabajo tomó nota de las recomendaciones del informe del grupo de trabajo de 2021 y del informe del Grupo de Expertos Gubernamentales de 2021, respectivamente:

i) "Durante todo el proceso del grupo de trabajo, los Estados participaron de forma constante y activa, lo que dio lugar a un rico intercambio de opiniones. Gracias a este intercambio se presentaron perspectivas diversas, ideas nuevas y propuestas importantes, con las que no todos los Estados estuvieron necesariamente de acuerdo, como la posibilidad de establecer nuevas obligaciones jurídicamente vinculantes. Las diversas perspectivas se reflejan en el anexo al resumen de la Presidencia de los debates y las propuestas específicas de texto a incluir en relación con el tema del programa titulado "Reglas, normas y principios". Estas perspectivas deberían seguir considerándose en futuros procesos de las Naciones Unidas, incluido el Grupo de Trabajo de Composición Abierta establecido en virtud de la resolución 75/240 de la Asamblea General"[40];

ii) "El Grupo observa que el derecho internacional humanitario solo se aplica en situaciones de conflicto armado. En este sentido, recuerda los principios jurídicos internacionales establecidos, incluidos, en su caso, los principios de humanidad, necesidad, proporcionalidad y distinción que se señalaron en el informe de 2015. El Grupo reconoció la necesidad de seguir estudiando cómo y cuándo se aplican estos principios al uso de las TIC por parte de los Estados y subraya que recordar estos principios no legitima ni fomenta en absoluto los conflictos"[41].

37. En los debates del grupo de trabajo centrados en la aplicación del derecho internacional al uso de las TIC, los Estados, entre otras cosas:

a) Reafirmaron los principios de soberanía e igualdad soberana de los Estados[42]. Por otra parte, los Estados reafirmaron que la soberanía de los Estados y las normas y principios internacionales que de ella dimanaban eran aplicables a la realización de actividades relacionadas con las TIC por los Estados y a su jurisdicción sobre la infraestructura de esas tecnologías que se hallara en su territorio. Las obligaciones existentes en virtud del derecho internacional eran aplicables a las actividades de los Estados relacionadas con las TIC. Los Estados ejercían jurisdicción sobre la infraestructura de las TIC en su territorio, entre otras cosas, estableciendo políticas y leyes y creando los mecanismos necesarios para proteger la infraestructura de las TIC en su territorio frente a las amenazas relacionadas con las TIC[43];

b) Reafirmaron el Artículo 2 3) de la Carta de las Naciones Unidas, según el cual "[l]os Miembros de la Organización arreglarán sus controversias internacionales

[40] Informe del grupo de trabajo de 2021 (A/75/816), anexo I, párr. 80.
[41] Informe del Grupo de Expertos Gubernamentales de 2021 (A/76/135), párr. 71 f), y resolución 76/19 de la Asamblea General, aprobada por consenso.
[42] Segundo informe anual sobre los progresos realizados, párr. 30 a).
[43] Informe del Grupo de Expertos Gubernamentales de 2021 (A/76/135), párr. 71 b), y resolución 76/19 de la Asamblea General, aprobada por consenso.

por medios pacíficos de tal manera que no se ponga en peligro ni la paz y la seguridad internacionales ni la justicia”[44], y el Artículo 33 1) de la Carta, según el cual “[l]as partes en una controversia cuya continuación sea susceptible de poner en peligro el mantenimiento de la paz y la seguridad internacionales tratarán de buscarle solución, ante todo, mediante la negociación, la investigación, la mediación, la conciliación, el arbitraje, el arreglo judicial, el recurso a organismos o acuerdos regionales u otros medios pacíficos de su elección”[45];

c) Reafirmaron el Artículo 2 4) de la Carta de las Naciones Unidas, según el cual “[l]os Miembros de la Organización, en sus relaciones internacionales, se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas”;

d) Reafirmaron también que, de conformidad con el principio de no intervención, los Estados no deben intervenir directa ni indirectamente en los asuntos internos de otro Estado, incluso por medio de las TIC[46];

e) Además, destacaron que los usos de las TIC que no contravenían la prohibición de la amenaza o el uso de la fuerza podían, según las circunstancias, ser contrarios a otros principios del derecho internacional, como la soberanía de los Estados o la prohibición de intervenir en los asuntos internos y externos de los Estados.

38. Los Estados también formularon otras propuestas concretas y orientadas a la acción en materia de derecho internacional, a saber:

a) Los Estados observaron los debates sobre derecho internacional celebrados en los períodos de sesiones sexto, séptimo y octavo y en las reuniones entre períodos de sesiones del grupo de trabajo y agradecieron que en dichos debates hubieran participado cada vez más Estados. Observando que durante la labor del grupo de trabajo se había profundizado mucho en esos debates sobre derecho internacional, los Estados propusieron que los debates pudieran seguir contando con sesiones informativas de expertos, por ejemplo, de la Comisión de Derecho Internacional o del mundo académico, según procediera, teniendo debidamente en cuenta la representación geográfica equitativa y los contextos nacionales;

b) Reafirmando que el derecho internacional, en particular la Carta de las Naciones Unidas, era aplicable y esencial para mantener la paz y la estabilidad y promover un entorno de TIC abierto, seguro, estable, accesible y pacífico[47], los Estados propusieron que el grupo de trabajo debatiera más a fondo la forma de aplicar el derecho internacional al uso de las TIC en relación con las especificidades del entorno de las TIC;

c) Los Estados señalaron además que el intercambio de puntos de vista y posturas nacionales sobre el derecho internacional podría contribuir a crear un entendimiento común sobre la aplicación del derecho internacional en el uso de las TIC y alentaron encarecidamente a que se siguieran compartiendo voluntariamente esos puntos de vista y posturas nacionales, que podrían incluir declaraciones nacionales y prácticas de los Estados sobre la aplicación del derecho internacional en el uso de las TIC. Además, los estudios y dictámenes pertinentes de expertos jurídicos

[44] Artículo 2 3) de la Carta de las Naciones Unidas.
[45] Artículo 33 1) de la Carta de las Naciones Unidas.
[46] Informe del Grupo de Expertos Gubernamentales de 2021 (A/76/135), párr. 71 c), y resolución 76/19 de la Asamblea General, aprobada por consenso.
[47] Informe del grupo de trabajo de 2021, párr. 34.

internacionales también podían ayudar a los Estados a desarrollar esos entendimientos comunes[48];

d) Reconociendo las iniciativas existentes de creación de capacidad en el ámbito del derecho internacional, los Estados continuaron recalcando la urgente necesidad de proseguir esas labores de creación de capacidad, incluso con el objetivo de garantizar que todos los Estados pudieran participar en pie de igualdad en el desarrollo de entendimientos comunes sobre la aplicación del derecho internacional en el uso de las TIC. Esas labores de creación de capacidad podrían incluir talleres, cursos de capacitación, conferencias e intercambios de las mejores prácticas a nivel internacional, interregional, regional y subregional, así como aprovechar las experiencias de las organizaciones regionales pertinentes, según procediera, y deberían llevarse a cabo de conformidad con los principios de creación de capacidad que figuraban en el párrafo 56 del informe del grupo de trabajo de 2021[49];

e) Tomando nota de la posibilidad de elaborar obligaciones vinculantes adicionales, si procediera, los Estados debatieron la necesidad de considerar si existían lagunas en la aplicación del derecho internacional vigente en el uso de las TIC y de seguir estudiando la elaboración de obligaciones jurídicamente vinculantes adicionales[50].

Próximas medidas recomendadas

39. **Se recomienda a los Estados que sigan participando en el grupo de trabajo en debates centrados sobre la aplicación del derecho internacional en el uso de las TIC a partir de los temas de la lista no exhaustiva de los párrafos 36 a 38 del presente anexo, así como de las propuestas sobre el tema del derecho internacional que figuran en el informe del grupo de trabajo de 2021 y el resumen de la Presidencia, según proceda.**

40. **Sobre la base de los debates de los períodos de sesiones sexto, séptimo y octavo del grupo de trabajo, se invita a los Estados a que sigan compartiendo voluntariamente sus puntos de vista y posturas nacionales, que pueden incluir declaraciones nacionales y prácticas de los Estados, sobre la aplicación del derecho internacional en el uso de las TIC. Se solicita a la Secretaría de las Naciones Unidas que publique esos puntos de vista en el sitio web del grupo de trabajo para referencia de todos los Estados y para que el grupo de trabajo pueda seguir debatiéndolos en sus siguientes períodos de sesiones.**

41. **Se recomienda a los Estados que estén en condiciones de hacerlo que sigan apoyando, de forma neutral y objetiva, en particular dentro de las Naciones Unidas, más iniciativas para desarrollar la capacidad en la esfera del derecho internacional, a fin de que todos los Estados contribuyan a generar entendimientos comunes del modo en que el derecho internacional es aplicable al uso de las TIC y para contribuir a crear consenso en la comunidad internacional. Esas labores de creación de capacidad deberían llevarse a cabo de acuerdo con los principios de creación de capacidad contenidos en el párrafo 56 del informe del grupo de trabajo de 2021.**

E. Medidas de fomento de la confianza

42. Durante los períodos de sesiones sexto, séptimo y octavo y las reuniones específicas entre períodos de sesiones del grupo de trabajo, los Estados continuaron

[48] Segundo informe anual sobre los progresos realizados, párr. 31 b).
[49] Segundo informe anual sobre los progresos realizados, párr. 31 c).
[50] Segundo informe anual sobre los progresos realizados, párr. 32.

debatiendo sobre las medidas de fomento de la confianza. Reafirmando el marco acumulativo y evolutivo de comportamiento responsable de los Estados en el uso de las TIC, los Estados hicieron propuestas concretas y orientadas a la acción sobre las medidas de fomento de la confianza. A continuación se presenta una lista no exhaustiva de propuestas con distintos niveles de apoyo por parte de los Estados, que pueden ser desarrolladas y complementadas en los próximos períodos de sesiones del grupo de trabajo:

a) Los Estados siguieron insistiendo en que las medidas de fomento de la confianza eran esenciales para incrementar la confianza y la previsibilidad entre los Estados y para reducir las tensiones, los malentendidos y los errores de cálculo. Los Estados también recalcaron las interrelaciones que existían entre las medidas de fomento de la confianza y otros aspectos del marco de comportamiento responsable de los Estados en el uso de las TIC;

b) Los Estados acogieron con satisfacción que el 9 de mayo de 2024 se hubiera puesto en marcha el Directorio Mundial de Puntos de Contacto y celebrado la primera reunión de los puntos de contacto. Los Estados también expresaron aprecio por la primera prueba de *ping* (envío de señales) del Directorio, que la Secretaría había iniciado el 10 de junio de 2024. Los Estados recordaron los propósitos y principios del Directorio, enunciados en el anexo A del segundo informe anual sobre los progresos realizados[51], y señalaron que el Directorio podría respaldar el avance de las medidas de fomento de la confianza en general. A ese respecto, los Estados pusieron de relieve la necesidad de seguir trabajando para desarrollar y poner en funcionamiento el Directorio en los siguientes períodos de sesiones del grupo de trabajo y, posteriormente, bajo los auspicios del futuro mecanismo permanente;

c) Los Estados destacaron que podría adoptarse un enfoque gradual para desarrollar el Directorio Mundial de Puntos de Contacto en función de la experiencia extraída de su puesta en funcionamiento. Se alentó a todos los Estados Miembros de las Naciones Unidas que aún no lo hubieran hecho a que designaran a sus puntos de contacto nacionales con carácter prioritario y lo antes posible. Con medidas como concienciar de la importancia de los puntos de contacto para la seguridad de las TIC en el contexto político nacional y crear capacidades específicas se podría contribuir a que el mayor número posible de Estados designara un punto de contacto para el Directorio. El grupo de trabajo alentó a los Estados que estuvieran en condiciones de hacerlo a que ayudaran a los puntos de contacto de los países en desarrollo a asistir en persona a las reuniones de puntos de contacto del grupo de trabajo;

d) Los Estados propusieron que, para optimizar la comunicación entre Estados a través del Directorio Mundial de Puntos de Contacto, podrían diseñarse plantillas normalizadas a fin de aumentar la claridad y la puntualidad de las comunicaciones. Al mismo tiempo, los Estados señalaron que esas plantillas deberían ser flexibles y voluntarias para no entorpecer innecesariamente el uso del Directorio, en especial en situaciones de urgencia;

e) Además de las medidas de fomento de la confianza ya recomendadas en anteriores informes de las Naciones Unidas, incluido el anexo B del segundo informe anual sobre los progresos realizados, titulado “Lista inicial de medidas globales voluntarias de fomento de la confianza”, los Estados propusieron otras medidas de fomento de la confianza globales, las cuales se recogen en el anexo B del presente informe;

f) Los Estados propusieron compartir los puntos de vista nacionales sobre la terminología técnica de las TIC como modo de mejorar la transparencia y la

[51] A/78/265.

comprensión entre los Estados. Los Estados podrían seguir compartiendo sus puntos de vista sobre la terminología técnica;

g) Se propuso que algunos aspectos del fomento de la confianza siguieran incluyendo el establecimiento de contacto con otras partes interesadas, como las empresas, las organizaciones no gubernamentales y los círculos académicos, cuando procediera[52];

h) Los Estados siguieron insistiendo en que el propio grupo de trabajo servía de medida de fomento de la confianza, pues proporcionaba un foro para debatir cuestiones sobre las que había acuerdo y cuestiones sobre las que aún no lo había[53]. Además, los Estados destacaron que el grupo de trabajo podría servir de plataforma para practicar medidas de fomento de la confianza innovadoras.

Próximas medidas recomendadas

43. **Se recomienda a los Estados que sigan intercambiando puntos de vista en el grupo de trabajo a propósito del desarrollo y la aplicación de las medidas de fomento de la confianza, incluido el posible desarrollo de medidas de fomento de la confianza adicionales, teniendo en cuenta los párrafos 42 a) a h) del presente anexo.**

44. **Se recomienda a los Estados que sigan desarrollando y poniendo en funcionamiento el Directorio Mundial de Puntos de Contacto en los próximos períodos de sesiones del grupo de trabajo y, posteriormente, bajo los auspicios del futuro mecanismo permanente. Se alienta a todos los Estados Miembros de las Naciones Unidas que aún no lo hayan hecho a que designen a sus puntos de contacto nacionales para el Directorio con carácter prioritario y lo antes posible. Además, se alienta a los Estados que estén en condiciones de hacerlo a que ayuden a los puntos de contacto de los países en desarrollo a asistir en persona a las reuniones de puntos de contacto del grupo de trabajo.**

45. **Se alienta a los Estados a que participen activamente en las pruebas de *ping* semestrales de los puntos de contacto previstas en el anexo A del segundo informe anual sobre los progresos realizados[54].**

46. **En consonancia con el anexo A del segundo informe anual sobre los progresos realizados[55], se alienta a la Presidencia del grupo de trabajo a que prepare un simulacro, en formato híbrido, en colaboración con los Estados y entidades de las Naciones Unidas interesados y con el apoyo de la Secretaría de las Naciones Unidas.**

47. **Se recomienda a los Estados que optimicen la comunicación a través del Directorio Mundial de Puntos de Contacto, en particular diseñando plantillas normalizadas para que los Estados las utilicen a su discreción. A ese respecto, se solicita a la Secretaría de las Naciones Unidas que, a partir de las aportaciones de los Estados y de la experiencia de las organizaciones regionales que proceda, prepare un ejemplo de plantilla antes de abril de 2025, con vistas a formular una recomendación consensuada.**

48. **Recordando la lista de medidas globales de fomento de la confianza contenida en el anexo B del segundo informe anual sobre los progresos realizados[56], los Estados recomiendan que las medidas de fomento de la confianza**

[52] Segundo informe anual sobre los progresos realizados, párr. 37 f).
[53] Segundo informe anual sobre los progresos realizados, párr. 37 g).
[54] Párr. 8.
[55] Párr. 13 e).
[56] A/78/265.

contenidas en el anexo B del presente informe sean medidas adicionales de fomento de la confianza globales y voluntarias, reconociendo que los Estados pueden aplicarlas según sus diferentes prioridades y capacidades nacionales. Se solicita a la Presidencia del grupo de trabajo que facilite la continuación de los debates sobre las formas de desarrollar, ampliar y poner en práctica esas medidas de fomento de la confianza, entre otras cosas, mediante: a) la creación de capacidad al respecto, y b) el Directorio Mundial de Puntos de Contacto.

49. **Se alienta a los Estados a que sigan compartiendo de forma voluntaria sus puntos de vista nacionales sobre la terminología técnica de las TIC para mejorar la transparencia y la comprensión entre los Estados[57].**

F. Creación de capacidad

50. Durante los períodos de sesiones sexto, séptimo y octavo y las reuniones específicas entre períodos de sesiones del grupo de trabajo, los Estados continuaron debatiendo sobre la creación de capacidad en materia de TIC en el contexto de la seguridad internacional. En esos períodos de sesiones, los Estados pusieron en común sus experiencias nacionales de cooperación internacional y creación de capacidad, así como las iniciativas bilaterales, regionales y mundiales en curso orientadas a crear capacidad en materia de TIC en el contexto de la seguridad internacional. Reafirmando el marco acumulativo y evolutivo del comportamiento responsable de los Estados en el uso de las TIC, los Estados hicieron propuestas concretas y orientadas a la acción sobre los esfuerzos de creación de capacidad en relación con las TIC en el contexto de la seguridad internacional. A continuación se presenta una lista no exhaustiva de propuestas con distintos niveles de apoyo por parte de los Estados, que pueden ser desarrolladas y complementadas en los próximos períodos de sesiones del grupo de trabajo:

a) Recordando y reafirmando los principios de creación de capacidad sobre la seguridad de las TIC aprobados en el informe del grupo de trabajo de 2021, los Estados siguieron destacando la necesidad de redoblar los esfuerzos para incorporar esos principios en los programas de creación de capacidad pertinentes. Además, los Estados siguieron alentando los esfuerzos para promover la creación de capacidad que respondiera a las cuestiones de género, como, por ejemplo, mediante la integración de una perspectiva de género en las políticas nacionales de TIC y de creación de capacidad, así como mediante la elaboración de listas de comprobación o cuestionarios para determinar las necesidades y lagunas en ese ámbito[58];

b) Haciendo hincapié en que la creación de capacidad no se ajustaba a una única solución, los Estados propusieron que los esfuerzos para adaptar la creación de capacidad a las necesidades de cada Estado receptor, que podían abarcar la transferencia de conocimientos, habilidades y tecnología de mutuo acuerdo, podrían mejorarse si cada Estado evaluaba su propio estado de seguridad de las TIC a nivel nacional. De esa forma sería posible detectar lagunas y ayudar a establecer objetivos claros y alcanzables en relación con la observancia y la adhesión al marco acumulativo y evolutivo de comportamiento responsable de los Estados en el uso de las TIC. Los Estados también subrayaron la necesidad de aumentar la oferta de programas de creación de capacidad y liderazgo en materia de seguridad de las TIC dirigidos a altos funcionarios y decisores nacionales. A ese respecto, los Estados siguieron subrayando el valor de la cooperación Sur-Sur, triangular y subregional

[57] Segundo informe anual sobre los progresos realizados, párr. 42.
[58] Segundo informe anual sobre los progresos realizados, párr. 43 a).

y regional, la cual no era un sustituto, sino un complemento, de la cooperación Norte-Sur;

c) Los Estados continuaron debatiendo la iniciativa de desarrollar un Portal Mundial de Cooperación para la Ciberseguridad y propusieron que fuera práctico y neutral, impulsado por los Estados Miembros y una plataforma modular de ventanilla única para los Estados desarrollada bajo los auspicios de las Naciones Unidas. Se preveía que el portal podría servir de plataforma de coordinación entre los Estados sobre cuestiones de seguridad de las TIC y ser lo bastante flexible como para evolucionar a la vez que las necesidades de los Estados en lo tocante al marco de comportamiento responsable en el uso de las TIC decidido por los Estados. Además, el portal podría armonizarse con otros portales en línea análogos. Posteriormente, el portal apoyaría y facilitaría la labor del futuro mecanismo permanente y buscaría complementar y no duplicar las iniciativas existentes;

d) También se propuso confeccionar un catálogo de creación de capacidad en materia de seguridad de las TIC en función de las necesidades para ayudar a los Estados a determinar sus necesidades de creación de capacidad y a acceder a información sobre cómo solicitar programas de creación de capacidad. Dicho catálogo también podría incorporarse al Portal Mundial de Cooperación para la Ciberseguridad si ambas iniciativas fueran establecidas por los Estados;

e) Los Estados se mostraron satisfechos con la mesa redonda mundial de alto nivel sobre la creación de capacidad en materia de TIC en el contexto de la seguridad internacional que había tenido lugar el 10 de mayo de 2024 en Nueva York. La mesa redonda había aportado valor a los debates del grupo de trabajo al concienciar sobre la urgencia de crear capacidad en materia de TIC entre los altos funcionarios públicos, mientras que las mesas redondas con profesionales de la creación de capacidad habían contribuido a fomentar el intercambio de información y mejores prácticas sobre cuestiones de creación de capacidad orientadas a la acción. Los Estados propusieron que se siguieran celebrando periódicamente mesas redondas sobre la creación de capacidad en materia de TIC en el contexto de la seguridad internacional;

f) Los Estados expresaron reconocimiento por el análisis[59] para estudiar el panorama de los programas e iniciativas de creación de capacidad dentro y fuera de las Naciones Unidas y a escala mundial y regional realizado por la Secretaría de las Naciones Unidas. A ese respecto, los Estados subrayaron que convendría coordinar más los esfuerzos de creación de capacidad en materia de seguridad de las TIC y que las Naciones Unidas podían desempeñar un papel importante en ellos. Los Estados señalaron que esos esfuerzos debían evitar duplicar iniciativas similares. Al mismo tiempo, si bien se expresó aprecio por los cauces de financiación existentes para crear capacidad en materia de TIC en el contexto de la seguridad internacional, se propuso que los Estados siguieran estudiando cauces de financiación adicionales bajo los auspicios del futuro mecanismo permanente sobre la seguridad de las TIC en el contexto de la seguridad internacional, incluso mediante la coordinación con los programas de desarrollo existentes y los mecanismos de financiación pertinentes;

g) Los Estados reconocieron que el propio grupo de trabajo podría ser una plataforma inclusiva para seguir intercambiando puntos de vista e ideas relacionadas con los esfuerzos de creación de capacidad en materia de seguridad de las TIC, incluida la mejor manera de aprovechar las iniciativas existentes con el fin de apoyar a los Estados en el desarrollo de la fuerza y la capacidad institucionales necesarias para aplicar el marco de comportamiento responsable de los Estados en el uso de las TIC. Los Estados subrayaron que el grupo de trabajo también podría utilizarse como plataforma para compartir las mejores prácticas de creación de capacidad en materia

[59] A/AC.292/2024/2.

de seguridad de las TIC y para seguir trabajando en la formulación de mecanismos de cooperación para hacer frente a las amenazas que planteaba el uso de las TIC. Se señaló que con ello deberían complementarse las actividades que ya se estaban llevando a cabo en otras partes del sistema de las Naciones Unidas;

h) Por medio del grupo de trabajo, entre otros medios, los Estados podrían seguir reforzando la coordinación y la cooperación entre los Estados y otras partes interesadas, como las empresas, las organizaciones no gubernamentales y los círculos académicos. Los Estados destacaron que también se podría implicar a los jóvenes en la labor del grupo de trabajo. Los Estados señalaron que otras partes interesadas, como las empresas, las organizaciones no gubernamentales y el mundo académico, ya desempeñaban un papel importante al colaborar con los Estados, en particular con fines de capacitación e investigación. Esas otras partes interesadas, a saber, las empresas, las organizaciones no gubernamentales y el mundo académico, podrían aprovechar la labor del grupo de trabajo en materia de creación de capacidad y hacer observaciones sobre esos esfuerzos;

i) Los Estados reafirmaron la importancia de la creación de capacidad no solo como cuestión transversal de la labor del grupo de trabajo, sino también como herramienta para concienciar y facilitar entendimientos comunes sobre el marco del comportamiento responsable de los Estados en el uso de las TIC.

Próximas medidas recomendadas

51. **Se recomienda a los Estados que sigan intercambiando puntos de vista en el grupo de trabajo sobre la creación de capacidad en materia de TIC en el contexto de la seguridad internacional, en particular en relación con los párrafos 50 a) a i) del presente anexo.**

52. **Se solicita a la Secretaría de las Naciones Unidas que prepare un informe inicial que contenga una propuesta para diseñar y poner en funcionamiento un portal mundial de cooperación y creación de capacidad en materia de seguridad de las TIC, teniendo en cuenta las iniciativas conexas, con miras a optimizar las sinergias y evitar duplicaciones, y que lo someta al examen del grupo de trabajo. Se invita a los Estados a que presenten sus opiniones sobre el diseño del portal, el cual deberá: a) ser práctico y neutral, impulsado por los Estados Miembros y una plataforma modular de ventanilla única para los Estados desarrollada bajo los auspicios de las Naciones Unidas; b) ser un repositorio de las opiniones y documentos de trabajo presentados por los Estados sobre temas relacionados con la seguridad en el uso de las TIC e incluir un calendario de eventos relacionados con la seguridad en el uso de las TIC; y c) incorporar un catálogo de creación de capacidad en materia de seguridad de las TIC en función de las necesidades, aprovechando el trabajo realizado en portales existentes, cuando proceda, para ayudar a los Estados a determinar sus necesidades de creación de capacidad y acceder a la información sobre los recursos disponibles para atenderlas. Se solicita a la Secretaría de las Naciones Unidas que prepare el informe inicial basándose en las opiniones de los Estados y en los puntos a) a c) del presente párrafo y que lo presente a tiempo para que pueda estudiarse en el décimo período de sesiones sustantivo del grupo de trabajo, en marzo de 2025. Posteriormente, el portal apoyaría y facilitaría la labor del futuro mecanismo permanente.**

53. **A fin de seguir prestando atención a la urgente cuestión de la creación de capacidad en materia de seguridad de las TIC, se recomienda a los Estados que celebren periódicamente mesas redondas mundiales de alto nivel sobre la creación de capacidad en materia de seguridad de las TIC, bajo los auspicios del futuro mecanismo permanente, para favorecer debates estratégicos y orientados**

a la acción sobre la creación de capacidad en el contexto de la seguridad de las TIC. Esas reuniones de alto nivel podrían incluir a profesionales de la creación de capacidad, así como a representantes de los Estados interesados y otras partes interesadas, como las empresas, las organizaciones no gubernamentales y los círculos académicos, teniendo debidamente en cuenta la representación geográfica equitativa. Se alienta a los Estados que estén en condiciones de hacerlo a que ayuden a los representantes y expertos de los países en desarrollo a asistir a las mesas redondas.

54. **Se recomienda a los Estados que sigan estudiando la creación de un fondo de contribuciones voluntarias de las Naciones Unidas, aprovechando al máximo las iniciativas existentes, para apoyar la creación de capacidad de los Estados en materia de seguridad en el uso de las TIC. El fondo facilitaría, entre otras cosas, la participación de representantes y expertos nacionales, en particular de países en desarrollo, en las reuniones pertinentes del futuro mecanismo permanente sobre seguridad de las TIC en el contexto de la seguridad internacional y serviría a otros objetivos señalados por los Estados. Se solicita a la Secretaría de las Naciones Unidas que prepare un informe inicial que contenga una propuesta para diseñar y poner en funcionamiento ese fondo de contribuciones voluntarias y lo someta al examen del grupo de trabajo y de los Estados a tiempo para que pueda estudiarse en el décimo período de sesiones sustantivo del grupo de trabajo, en marzo de 2025, con miras a que se formule una recomendación consensuada sobre esos detalles a más tardar en julio de 2025 y a que el fondo se ponga en funcionamiento bajo los auspicios del futuro mecanismo permanente. Se solicita también a la Secretaría de las Naciones Unidas que, al preparar esa propuesta, aborde, entre otras cosas, las cuestiones relacionadas con la designación de un administrador adecuado para el fondo, los requisitos financieros y administrativos, la elegibilidad y el acceso de los potenciales beneficiarios a los fondos, el seguimiento y la evaluación, y la forma de incorporar los principios de creación de capacidad en materia de seguridad de las TIC en la implementación del fondo. Se solicita además a la Secretaría de las Naciones Unidas que busque complementar y no duplicar las iniciativas existentes y que base su labor en el objetivo de que el fondo pueda recibir financiación de fuentes públicas, privadas y filantrópicas.**

55. **Se invita a los Estados que estén en condiciones de hacerlo a que sigan apoyando los programas de creación de capacidad, incluso en colaboración, cuando proceda, con las organizaciones regionales y subregionales y otras partes interesadas, como las empresas, las organizaciones no gubernamentales y los círculos académicos.**

G. Diálogo institucional periódico

56. Durante los períodos de sesiones sexto, séptimo y octavo y las reuniones específicas entre períodos de sesiones del grupo de trabajo, los Estados continuaron debatiendo acerca del diálogo institucional periódico sobre la base de las recomendaciones formuladas en el segundo informe anual sobre los progresos realizados[60]. Reafirmando el marco acumulativo y evolutivo de comportamiento responsable de los Estados en el uso de las TIC, los Estados hicieron propuestas concretas y orientadas a la acción sobre el diálogo institucional periódico.

a) Partiendo de los objetivos enunciados en las resoluciones pertinentes de la Asamblea General, incluidas, entre otras, las resoluciones 78/16 y 78/237, en relación

[60] Párrs. 54 a 59.

con los debates sobre el diálogo institucional periódico celebrados en el seno del grupo de trabajo, y de las recomendaciones contenidas en el informe del grupo de trabajo de 2021[61] y en los informes anuales primero[62] y segundo[63] sobre los progresos realizados por el grupo de trabajo, los Estados profundizaron en los debates sobre los posibles elementos del futuro mecanismo permanente;

b) Los Estados expresaron su voluntad de proseguir los debates para consensuar la creación de un futuro mecanismo permanente de una sola vía. A ese respecto, los Estados examinaron el documento de la Presidencia relativo a los elementos del mecanismo permanente de composición abierta y orientado a la acción sobre la seguridad de las TIC en el contexto de la seguridad internacional, en el que figuraban elementos relacionados con los principios rectores, las funciones y el alcance, la estructura, las modalidades y los procesos decisorios del futuro mecanismo permanente.

57. Los Estados propusieron que el futuro mecanismo permanente facilitara que siguieran funcionando y desarrollándose todas las iniciativas existentes creadas bajo los auspicios del grupo de trabajo (2021-2025) u otros procesos anteriores, incluidos, entre otros, el Directorio Mundial de Puntos de Contacto y la mesa redonda mundial sobre la creación de capacidad en materia de seguridad de las TIC.

Próximas medidas recomendadas

58. **Los Estados recomiendan que el futuro mecanismo permanente se establezca en consonancia con los elementos de consenso contenidos en el documento relativo a los elementos del mecanismo permanente de composición abierta y orientado a la acción sobre la seguridad de las TIC en el contexto de la seguridad internacional, que figura en el anexo C del presente informe, con el fin de que la transición del grupo de trabajo al futuro mecanismo permanente sea fluida.**

59. **Se recomienda a los Estados que prosigan los debates en el seno del actual grupo de trabajo y formulen recomendaciones en el informe final del grupo de trabajo, que se aprobará en julio de 2025, acerca de: a) las modalidades de participación de otras partes interesadas, como las empresas, las organizaciones no gubernamentales y el mundo académico, en el futuro mecanismo permanente; b) los grupos temáticos específicos del futuro mecanismo permanente; y c) otros elementos necesarios.**

60. **Los Estados recomiendan que el futuro mecanismo permanente facilite que sigan funcionando y desarrollándose todas las iniciativas existentes creadas bajo los auspicios del grupo de trabajo (2021-2025) u otros procesos anteriores, incluidos, entre otros, el Directorio Mundial de Puntos de Contacto y la mesa redonda mundial sobre la creación de capacidad en materia de seguridad de las TIC.**

[61] Informe del grupo de trabajo de 2021 (A/75/816), anexo I, párr. 77.

[62] Primer informe anual sobre los progresos realizados, sección sobre el diálogo institucional periódico, próximas medidas recomendadas, párr. 2.

[63] Segundo informe anual sobre los progresos realizados, párrafos 54 a 59.

Anexo A

Lista voluntaria de medidas prácticas para aplicar las normas voluntarias y no vinculantes sobre el comportamiento responsable de los Estados en el uso de las TIC

1. En el segundo informe anual sobre los progresos realizados por el grupo de trabajo, los Estados propusieron la próxima medida recomendada siguiente: "[l]os Estados deben elaborar orientaciones adicionales, incluida una lista de comprobación, sobre la aplicación de las normas, teniendo en cuenta los acuerdos anteriores. Se solicita a la Presidencia del grupo de trabajo que elabore un borrador inicial de esta lista de comprobación para su consideración por parte de los Estados"[1].

2. Esta lista pretende ser una herramienta voluntaria de creación de capacidad que los Estados tal vez deseen utilizar como parte de sus esfuerzos para aplicar las normas voluntarias y no vinculantes sobre el comportamiento responsable de los Estados en el uso de las TIC. Los Estados reconocieron que la lista podría ser una herramienta útil de creación de capacidad para definir las capacidades mínimas que necesitaban los Estados para crear resiliencia en términos de seguridad de las TIC. En ese sentido, la lista podría: a) servir de punto de partida para apoyar los esfuerzos de aplicación de los Estados; b) constituir una herramienta de evaluación útil y ayudar a definir las prioridades en términos de esfuerzos de creación de capacidad adaptados; y c) funcionar como referencia común para facilitar el intercambio de las mejores prácticas en ámbitos específicos de la seguridad de las TIC. La lista es un documento en evolución que podría actualizarse periódicamente.

3. En general, aplicar las normas voluntarias y no vinculantes en su conjunto puede requerir que los Estados adopten algunas medidas prácticas comunes.

A nivel nacional, esas medidas podrían incluir:

a) La creación de Equipos de Respuesta a Emergencias Informáticas (EREI) o Equipos de Respuesta a Incidentes de Seguridad Informática (ERISI) y otras estructuras y mecanismos nacionales de coordinación;

b) La formulación de leyes y políticas nacionales en materia de TIC, incluida una estrategia nacional sobre TIC.

A nivel internacional, las medidas de los Estados para apoyar la aplicación de las normas podrían incluir:

a) La participación en procesos internacionales, interregionales, regionales y subregionales inclusivos relacionados con la seguridad de las TIC;

b) El intercambio de información y mejores prácticas sobre distintos aspectos de la seguridad de las TIC;

c) La prestación y la solicitud de asistencia para incidentes relacionados con las TIC, cuando proceda, utilizando cauces como el Directorio Mundial de Puntos de Contacto.

4. Crear capacidad es clave para que todos los Estados puedan adoptar esas medidas prácticas y, por tanto, es un pilar central para que las normas se apliquen a escala mundial. Al mismo tiempo, los Estados reconocen que la aplicación de las normas no se ajusta a una única solución, por lo que, al utilizar esta lista para aplicar

[1] Segundo informe anual sobre los progresos realizados por el actual grupo de trabajo (A/78/265), párr. 26.

las normas deberán tenerse en cuenta las diferencias técnicas entre los Estados, la diversidad de sistemas nacionales y las especificidades regionales.

5. Esta lista de medidas prácticas no es exhaustiva. El uso de esta lista por los Estados es completamente voluntario. Al confeccionar y utilizar esta lista, los Estados recuerdan y reafirman los acuerdos anteriores, que son los elementos que consolidan un marco acumulativo y evolutivo de comportamiento responsable de los Estados en el uso de las TIC[2].

[2] Los Estados reafirmaron los informes anuales de consenso primero y segundo sobre los progresos realizados por el actual grupo de trabajo (respectivamente, A/77/275 y A/78/265), el informe de consenso del grupo de trabajo de 2021 sobre los avances en la esfera de las TIC en el contexto de la seguridad internacional (A/75/816) y los informes de consenso de los Grupos de Expertos Gubernamentales de 2010, 2013, 2015 y 2021 (A/65/201, A/68/98, A/70/174 y A/76/135). Véase el segundo informe anual sobre los progresos realizados (A/78/265), párr. 3.

Norma a)
En consonancia con los propósitos de las Naciones Unidas, incluido el mantenimiento de la paz y la seguridad internacionales, los Estados deben cooperar en la formulación y aplicación de medidas para aumentar la estabilidad y la seguridad en el uso de las TIC y prevenir las prácticas relacionadas con esas tecnologías que se haya reconocido que son perjudiciales o que pueden entrañar amenazas a la paz y la seguridad internacionales.

Medidas voluntarias y prácticas para aplicar la norma

Medidas nacionales

☐ 1. Establecer o reforzar políticas y leyes nacionales y los procesos de revisión correspondientes para apoyar o facilitar la cooperación internacional[3].

☐ 2. Crear o apuntalar estructuras y mecanismos nacionales[4] para detectar incidentes relacionados con las TIC, defenderse de ellos o darles respuesta.

☐ 3. Establecer o reforzar acuerdos y políticas pangubernamentales de cooperación y asociación para apoyar o facilitar la cooperación internacional[5].

☐ 4. Establecer o reforzar acuerdos de cooperación y diálogo con el sector privado, el mundo académico, la sociedad civil y la comunidad técnica[6].

☐ 5. Realizar encuestas voluntarias sobre los esfuerzos nacionales para aplicar las normas y poner en común las experiencias al respecto[7]. Esto podría hacerse a través del informe del Secretario General sobre los avances en la esfera de las TIC en el contexto de la seguridad internacional, así como a través de la Encuesta Nacional de Implementación[8].

Medidas que requieren cooperación internacional

☐ 6. Participar, cuando proceda, en la labor de las organizaciones regionales y subregionales que fomentan la cooperación entre los Estados en torno al uso de las TIC en el contexto de la seguridad internacional[9].

---

[3] Informe del Grupo de Expertos Gubernamentales de 2021 (A/76/135), párr. 21, y resolución 76/19 de la Asamblea General, aprobada por consenso.

[4] A/76/135, párr. 21. Nota adicional: dichas estructuras y mecanismos podrían incluir un centro nacional o un organismo o entidad responsable que dirija las cuestiones de seguridad de las TIC o Equipos de Respuesta a Emergencias Informáticas (EREI) o Equipos de Respuesta a Incidentes de Seguridad Informática (ERISI).

[5] A/76/135, párr. 21.

[6] A/76/135, párr. 21.

[7] A/76/135, párr. 21.

[8] Primer informe anual sobre los progresos realizados por el grupo de trabajo (A/77/275), sección sobre las próximas medidas recomendadas respecto de las reglas, normas y principios de comportamiento responsable de los Estados, párr. 3.

[9] Reconociendo que no todos los Estados eran miembros de una organización regional y no todas las organizaciones regionales se centraban en la cuestión de la seguridad en el uso de las TIC, el grupo de trabajo señaló que los esfuerzos regionales eran complementarios a su labor (informes anuales primero y segundo sobre los progresos realizados por el grupo de trabajo (respectivamente, A/77/275, párr. 5, y A/78/265, párr. 7).

Otras medidas sugeridas

- Considerar la posibilidad de participar en mecanismos inclusivos y transparentes, como el Directorio Mundial de Puntos de Contacto, para fomentar la cooperación y el intercambio de información.

Norma b)
En el caso de incidentes relacionados con las TIC, los Estados deben tener en cuenta toda la información pertinente, incluido el contexto más amplio en el que se haya producido el hecho, los problemas que plantea la atribución en el entorno de estas tecnologías y la naturaleza y el alcance de las consecuencias.

Medidas voluntarias y prácticas para aplicar la norma

Medidas nacionales

☐ 1. Establecer o reforzar las estructuras, las políticas, los procesos, los marcos legislativos y los mecanismos de coordinación nacionales relacionados con las TIC pertinentes para evaluar la gravedad y replicabilidad de un incidente relacionado con las TIC. Esto puede abarcar asociaciones y otras formas de colaboración con las partes interesadas pertinentes[10].

☐ 2. Cuando ocurran incidentes relacionados con las TIC, tomar en consideración todos los aspectos al evaluar el incidente[11]. Esos aspectos, que han de basarse en hechos probados, pueden incluir:
- Las características técnicas del incidente;
- Su alcance, escala y efectos;
- El contexto más amplio, incluida la relación del incidente con la paz y la seguridad internacionales; y
- Los resultados de las consultas entre los Estados afectados[12].

☐ 3. Establecer procesos para responder a una actividad malintencionada relacionada con las TIC atribuible a otro Estado que sean conformes con las obligaciones que le incumben en virtud de la Carta de las Naciones Unidas y otras normas del derecho internacional, incluidas las relativas a la solución de controversias por medios pacíficos y a los hechos internacionalmente ilícitos[13].

Medidas que requieren cooperación internacional

☐ 4. Emprender cooperación entre los Equipos de Respuesta a Emergencias Informáticas (CERT)/Equipos de Respuesta a Incidentes de Seguridad Informática (ERISI) nacionales, las autoridades de los Estados competentes en materia de TIC y la comunidad diplomática a fin de fortalecer la capacidad de los Estados para detectar e investigar los incidentes malintencionados relacionados con las TIC y fundamentar sus preocupaciones y constataciones antes de llegar a una conclusión sobre un incidente[14].

☐ 5. Utilizar plataformas multilaterales, regionales, bilaterales y multipartitas para intercambiar prácticas y compartir información sobre enfoques nacionales de atribución, incluso sobre el modo en que distinguen entre distintos tipos de atribución, y sobre amenazas e incidentes relacionados con las TIC[15].

---

[10] A/76/135, párr. 26.

[11] La atribución es una operación compleja y deben tenerse en cuenta diversos factores antes de establecer el origen de un incidente relacionado con las TIC. Se pide cautela y que se estudie la posible aplicación del derecho internacional, para ayudar a evitar malentendidos y una escalada de tensiones entre los Estados (A/76/135, párr. 22).

[12] A/76/135, párr. 24.

[13] A/76/135, párr. 25.

[14] A/76/135, párr. 27.

[15] A/76/135, párr. 28.

☐ 6. Se alienta a todas las partes implicadas en un incidente relacionado con las TIC a que mantengan consultas por conducto de las autoridades competentes que procedan[16].

☐ 7. Establecer procesos de arreglo pacífico de controversias[17] respecto de incidentes relacionados con las TIC por medios como la negociación, la investigación, la mediación, la conciliación, el arbitraje, el arreglo judicial, el recurso a organismos o acuerdos regionales u otros medios pacíficos de su elección[18].

Otras medidas sugeridas

- Considerar la posibilidad de utilizar, cuando proceda, cauces de comunicación multilaterales de índole diplomática y técnica, como el Directorio Mundial de Puntos de Contacto, para intercambiar información y celebrar consultas entre Estados cuando ocurra un incidente relacionado con las TIC.

[16] A/76/135, párr. 23.
[17] A/76/135, párr. 25.
[18] Carta de las Naciones Unidas, Artículo 33 1).

Norma c)
Los Estados no deben permitir a sabiendas que su territorio sea utilizado para cometer hechos internacionalmente ilícitos utilizando TIC.

Medidas voluntarias y prácticas para aplicar la norma

Medidas nacionales

☐ 1. Ante la comisión de un hecho internacionalmente ilícito en su territorio, los Estados tomarán medidas razonables dentro de su capacidad para poner fin a la actividad que tiene lugar en su territorio por medios que sean proporcionados, apropiados y eficaces y de forma coherente con el derecho internacional e interno. No se espera que los Estados puedan o deban controlar todas las actividades relacionadas con las TIC que se realizan en su territorio[19].

☐ 2. Establecer y utilizar estructuras y mecanismos para formular y responder a las solicitudes de asistencia en el caso de un incidente relacionado con las TIC[20].

Medidas que requieren cooperación internacional

☐ 3. Si ocurre un incidente relacionado con las TIC, podrían adoptarse las medidas siguientes:
- Un Estado afectado por una actividad debe notificarla al Estado en el que se origina[21].
- El Estado notificado debe acusar recibo de la notificación para facilitar la cooperación y la clarificación de los hechos. El acuse de recibo de esta notificación no indica que se esté de acuerdo con la información contenida en ella[22].
- El Estado notificado debe hacer todos los esfuerzos razonables para contribuir a determinar si se ha cometido un hecho internacionalmente ilícito[23].

Otras medidas sugeridas

• Considerar la posibilidad de utilizar, cuando proceda, cauces de comunicación multilaterales de índole diplomática y técnica, como el Directorio Mundial de Puntos de Contacto, para intercambiar información y solicitar o responder a solicitudes de asistencia cuando ocurra un incidente relacionado con las TIC.

---

[19] A/76/135, párr. 30 a).

[20] Un Estado que sea consciente de que se están cometiendo hechos internacionalmente ilícitos utilizando TIC situadas en su territorio, pero carezca de la capacidad necesaria para hacerles frente, puede considerar la posibilidad de solicitar asistencia a otros Estados o al sector privado de forma coherente con el derecho internacional e interno. Los Estados deben actuar de buena fe y de conformidad con el derecho internacional al prestar asistencia y no aprovechar la oportunidad para realizar actividades malintencionadas contra el Estado que la solicita o contra un tercer Estado (informe del Grupo de Expertos Gubernamentales de 2021 (A/76/135), párr. 30 b)).

[21] A/76/135, párr. 30 c).

[22] A/76/135, párr. 30 c).

[23] A/76/135, párr. 30 c). El hecho de que un incidente relacionado con las TIC tenga su origen en el territorio o la infraestructura de un tercer Estado no implica, por sí mismo, la responsabilidad de ese Estado en el incidente. Además, la notificación a un Estado de que su territorio se está utilizando para realizar un hecho ilícito no implica, por sí misma, que sea responsable de ese hecho (informe del Grupo de Expertos Gubernamentales de 2021 (A/76/135), párr. 30 d), y segundo informe anual sobre los progresos realizados (A/78/265), anexo A, párr. 10).

Norma d)
Los Estados deben estudiar la mejor manera de cooperar para intercambiar información, prestarse asistencia mutua, enjuiciar la utilización de las TIC con fines terroristas y delictivos y aplicar otras medidas de cooperación para hacer frente a esas amenazas. Quizás los Estados deberían considerar si es necesario elaborar nuevas medidas a ese respecto.

Medidas voluntarias y prácticas para aplicar la norma

Medidas nacionales

☐ 1. Desarrollar protocolos y procedimientos apropiados para recopilar, manejar y almacenar las pruebas en línea relacionadas con la utilización de las TIC con fines delictivos y terroristas, lo que implica la gestión adecuada de la cadena de custodia, de conformidad con las obligaciones que imponga el derecho internacional[24].

☐ 2. Establecer políticas, legislación, estructuras y mecanismos nacionales que faciliten la cooperación transfronteriza en cuestiones técnicas, policiales, jurídicas y diplomáticas pertinentes para abordar la utilización de las TIC con fines delictivos y terroristas[25].

Medidas que requieren cooperación internacional

☐ 3. Reforzar y seguir desarrollando mecanismos que puedan facilitar los intercambios de información entre las organizaciones nacionales, regionales e internacionales pertinentes con el fin de aumentar la conciencia sobre la seguridad de las TIC entre los Estados y reducir el espacio operativo de las actividades terroristas y delictivas en línea[26].

☐ 4. Utilizar los procesos, iniciativas e instrumentos jurídicos existentes y considerar otros procedimientos o cauces de comunicación para facilitar el intercambio de información y asistencia a fin de hacer frente a la utilización de las TIC con fines delictivos y terroristas[27].

☐ 5. Proporcionar asistencia para las investigaciones de manera oportuna, garantizando que dichas acciones se lleven a cabo de conformidad con las obligaciones del Estado en virtud del derecho internacional[28].

[24] A/76/135, párr. 33.
[25] A/76/135, párr. 32.
[26] A/76/135, párr. 33.
[27] A/76/135, párr. 35.
[28] A/76/135, párr. 33.

Norma e)
Para garantizar la seguridad del uso de las TIC, los Estados deben acatar las resoluciones del Consejo de Derechos Humanos 20/8 y 26/13, relativas a la promoción, la protección y el disfrute de los derechos humanos en Internet, así como las resoluciones de la Asamblea General 68/167 y 69/166, relativas al derecho a la privacidad en la era digital, a fin de garantizar el pleno respeto de los derechos humanos, incluido el derecho a la libertad de expresión.

Medidas voluntarias y prácticas para aplicar la norma

Medidas nacionales

- ☐ 1. Los Estados deben respetar y proteger los derechos humanos y las libertades fundamentales, tanto en línea como fuera de ella, de acuerdo con sus respectivas obligaciones[29].
- ☐ 2. Tomar nota de la necesidad de abordar los nuevos retos y dilemas que han surgido en torno al uso de las TIC por los Estados que puedan tener efectos especialmente negativos en el ejercicio y el disfrute de los derechos humanos, en particular con arreglo a lo dispuesto en las nuevas resoluciones de la Asamblea General[30].
- ☐ 3. Considerar la posibilidad de promover e invertir en medidas técnicas y jurídicas a fin de orientar el desarrollo y el uso de las TIC de una manera más inclusiva y accesible y que no afecte negativamente a los miembros de comunidades o grupos individuales, teniendo en cuenta las consecuencias que las tecnologías nuevas y emergentes pueden tener para los derechos humanos y la seguridad de las TIC[31].
- ☐ 4. Colaborar con las partes interesadas que contribuyen de distintas maneras a la protección y promoción de los derechos humanos y las libertades fundamentales en línea y fuera de ella[32].

[29] A/76/135, párr. 36.
[30] A/76/135, párrs. 37 y 38.
[31] A/76/135, párr. 40.
[32] A/76/135, párr. 41.

Norma f)
Un Estado no debe realizar ni apoyar a sabiendas actividades en la esfera de las TIC contrarias a las obligaciones que le incumben en virtud del derecho internacional que dañen intencionadamente infraestructuras fundamentales o dificulten de otro modo la utilización y el funcionamiento de infraestructuras fundamentales que prestan servicios al público.

Medidas voluntarias y prácticas para aplicar la norma

Medidas nacionales

☐ 1. Determinar qué infraestructuras o sectores cada Estado considera críticos dentro de su jurisdicción, de conformidad con las prioridades nacionales y los métodos de categorización de las infraestructuras críticas[33].

☐ 2. Establecer las medidas políticas y legislativas pertinentes a nivel nacional para garantizar que las actividades de TIC realizadas o apoyadas por un Estado que puedan afectar a las infraestructuras críticas de otro Estado o a la prestación de servicios públicos esenciales en él se ajusten a esta norma, se lleven a cabo de conformidad con sus obligaciones jurídicas internacionales y estén sujetas a una revisión y supervisión exhaustivas[34].

Medidas que requieren cooperación internacional

☐ 3. Cooperar con otros Estados en la protección de infraestructuras críticas que prestan servicios a varios Estados, como la infraestructura técnica esencial para la integridad o disponibilidad general de Internet[35].

[33] A/76/135, párr. 44.
[34] A/76/135, párr. 46.
[35] A/76/135, párr. 45.

Norma g)
Los Estados deben tomar las medidas apropiadas para proteger las infraestructuras fundamentales frente a amenazas relacionadas con las TIC, teniendo en cuenta la resolución 58/199 de la Asamblea General.

Medidas voluntarias y prácticas para aplicar la norma

Medidas nacionales

☐ 1. Garantizar la seguridad y la protección de los productos de las TIC a lo largo de su ciclo de vida[36].

☐ 2. Clasificar los incidentes relacionados con las TIC en función de su escala y gravedad[37].

Medidas que requieren cooperación internacional

☐ 3. Fomentar la cooperación transfronteriza con los propietarios y operadores de las infraestructuras pertinentes para mejorar las medidas de seguridad de las TIC que se aplican a dichas infraestructuras y reforzar los procesos y procedimientos existentes o desarrollar otros complementarios a fin de detectar y mitigar los incidentes relacionados con las TIC que afecten a dichas infraestructuras[38].

Como parte de las medidas para aplicar la norma g), los Estados también podrían considerar la posibilidad de tener en cuenta la lista de elementos que figura en el anexo de la resolución 58/199 de la Asamblea General, relativa a la creación de una cultura mundial de seguridad cibernética y protección de las infraestructuras de información esenciales, como sigue:

☐ 1. Contar con redes de alerta de emergencia en relación con las vulnerabilidades, las amenazas y los incidentes informáticos.

☐ 2. Crear más conciencia para que los interesados entiendan la naturaleza y el alcance de sus infraestructuras de información esenciales y la función que debe desempeñar cada uno en su protección.

☐ 3. Examinar las infraestructuras y determinar las interdependencias de estas, mejorando así su protección.

☐ 4. Promover alianzas entre las partes interesadas, tanto públicas como privadas, para compartir y analizar las infraestructuras de información esenciales a fin de prevenir e investigar los daños y los ataques contra dichas infraestructuras, y responder a ellos.

☐ 5. Crear y mantener redes de comunicación para casos de crisis y probarlas para asegurarse de que seguirán siendo estables y seguras en situaciones de emergencia.

☐ 6. Garantizar que en las políticas sobre disponibilidad de datos se tenga en cuenta la necesidad de proteger las infraestructuras de información esenciales.

☐ 7. Facilitar el rastreo de los ataques contra las infraestructuras de información esenciales y, cuando corresponda, revelar la información recabada a otros Estados.

[36] A/76/135, párr. 50.
[37] A/76/135, párr. 50.
[38] A/76/135, párr. 49.

☐ 8. Ofrecer capacitación y hacer prácticas para mejorar las capacidades de respuesta y probar planes de continuidad y contingencia en el caso de un ataque contra las infraestructuras de información, y alentar a las partes interesadas a emprender actividades similares.

☐ 9. Contar con leyes sustantivas y de procedimiento adecuadas y personal capacitado para que los Estados puedan investigar los ataques contra las infraestructuras de información esenciales y enjuiciar a los responsables, y coordinar dichas investigaciones con otros Estados, cuando corresponda.

☐ 10. Cooperar a nivel internacional, cuando corresponda, para proteger las infraestructuras de información esenciales, en particular desarrollando y coordinando sistemas de alerta de emergencia, compartiendo y analizando información sobre vulnerabilidades, amenazas e incidentes y coordinando las investigaciones sobre los ataques contra dichas infraestructuras de conformidad con las leyes nacionales.

☐ 11. Promover la investigación y el desarrollo a nivel nacional e internacional y alentar la aplicación de tecnologías de seguridad que cumplan las normas internacionales.

Otras medidas sugeridas

- Considerar la posibilidad de determinar las medidas estructurales, técnicas, institucionales, legislativas y reglamentarias y los planes de contingencia que sean necesarios para proteger las infraestructuras críticas nacionales y restablecer su funcionamiento en caso de incidente.

Norma h)
Los Estados deben atender las solicitudes de asistencia apropiadas de otro Estado cuyas infraestructuras fundamentales sean objeto de actos malintencionados en los que se empleen TIC. Los Estados también deben atender las solicitudes apropiadas para mitigar toda actividad malintencionada relacionada con las TIC originada en su territorio que esté dirigida contra infraestructuras fundamentales de otro Estado, teniendo debidamente en cuenta la soberanía.

Medidas voluntarias y prácticas para aplicar la norma

Medidas nacionales

☐ 1. Disponer de las estructuras y mecanismos nacionales necesarios para detectar y mitigar los incidentes relacionados con las TIC que puedan amenazar la paz y la seguridad internacionales[39].

Medidas que requieren cooperación internacional

☐ 2. Cuando sea necesario para mitigar toda actividad malintencionada relacionada con las TIC que esté dirigida contra infraestructuras críticas e infraestructuras críticas de información, recabar u ofrecer asistencia de forma bilateral o a través de acuerdos regionales o internacionales, con el debido respeto a la soberanía[40].

☐ 3. Solicitar los servicios del sector privado para ayudar a responder a las solicitudes de asistencia, cuando proceda[41].

☐ 4. Participar en mecanismos de cooperación que definan los medios y el modo de las comunicaciones en casos de crisis relacionadas con las TIC y de la gestión y resolución de los incidentes, incluso estableciendo procesos, procedimientos y plantillas comunes y transparentes[42].

Otras medidas sugeridas

- Considerar la posibilidad de utilizar, cuando proceda, cauces de comunicación multilaterales de índole diplomática y técnica, como el Directorio Mundial de Puntos de Contacto, para intercambiar información y solicitar o responder a solicitudes de asistencia cuando ocurra un incidente relacionado con las TIC.

[39] A/76/135, párr. 53. Nota adicional: dichas estructuras y mecanismos podrían incluir un centro nacional o un organismo o entidad responsable que dirija las cuestiones de seguridad de las TIC o Equipos de Respuesta a Emergencias Informáticas (EREI) o Equipos de Respuesta a Incidentes de Seguridad Informática (ERISI).

[40] A/76/135, párrs. 51 y 52.

[41] A/76/135, párr. 52.

[42] A/76/135, párrs. 54 y 55.

Norma i)
Los Estados deben adoptar 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 las TIC. Los Estados deben tratar de evitar la proliferación de técnicas e instrumentos malignos en la esfera de las TIC, así como el uso de funciones ocultas perniciosas.

Medidas voluntarias y prácticas para aplicar la norma

Medidas nacionales

- ☐ 1. Poner en marcha a nivel nacional marcos y mecanismos integrales, transparentes, objetivos e imparciales para la gestión del riesgo en la cadena de suministro, en consonancia con las obligaciones internacionales del Estado, teniendo en cuenta una serie de factores, incluidos los beneficios y riesgos de las nuevas tecnologías[43].
- ☐ 2. Establecer políticas y programas para promover objetivamente la adopción de buenas prácticas por parte de los proveedores y vendedores de equipos y sistemas de TIC con el fin de fomentar la confianza internacional en la integridad y la seguridad de los productos y servicios de las TIC, mejorar la calidad y promover la elección[44].
- ☐ 3. Establecer medidas para mejorar la integridad de la cadena de suministro, incluso exigiendo a los proveedores de TIC que incorporen la seguridad y la protección en el diseño, el desarrollo y todo el ciclo de vida de los productos de las TIC. Considerar la posibilidad de establecer procesos de certificación independientes e imparciales[45].
- ☐ 4. Establecer salvaguardias legislativas y de otro tipo que mejoren la protección de los datos y la privacidad[46].
- ☐ 5. Establecer medidas que prohíban la introducción de funciones ocultas perniciosas y la explotación de vulnerabilidades en los productos de las TIC que puedan poner en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas y las redes, incluso en las infraestructuras críticas[47].
- ☐ 6. Reforzar las alianzas con el sector privado para mejorar en colaboración la seguridad de las TIC y de su uso. Seguir alentando al sector privado a desempeñar un papel adecuado para mejorar la seguridad de las TIC y de su uso, incluida la seguridad de la cadena de suministro de productos de las TIC, de conformidad con las leyes y normativas nacionales de los países en los que operan[48].

[43] A/76/135, párr. 57 a).
[44] Segundo informe anual sobre los progresos realizados (A/78/265), párr. 23 d).
[45] A/76/135, párr. 58 a).
[46] A/76/135, párr. 58 b).
[47] A/76/135, párr. 58 c).
[48] Segundo informe anual sobre los progresos realizados (A/78/265), párr. 23 e).

Medidas que requieren cooperación internacional

- ☐ 7. Prestar mayor atención en el ámbito de la política nacional y en el diálogo con los Estados y los actores pertinentes en el marco de las Naciones Unidas y otros foros al modo de garantizar que todos los Estados puedan competir e innovar en igualdad de condiciones, a fin de permitir la plena realización del potencial de las TIC para aumentar el desarrollo social y económico mundial y contribuir al mantenimiento de la paz y la seguridad internacionales, al tiempo que se salvaguardan la seguridad nacional y el interés público[49].

- ☐ 8. Participar en procesos multilaterales inclusivos y transparentes sobre medidas de cooperación tales como intercambios de buenas prácticas sobre la gestión de riesgos en la cadena de suministro, el desarrollo y la aplicación de reglas y normas comunes interoperables a nivel mundial para la seguridad de la cadena de suministro, y otros enfoques destinados a disminuir las vulnerabilidades de la cadena de suministro[50].

[49] A/76/135, párr. 57 c).
[50] Segundo informe anual sobre los progresos realizados (A/78/265), párr. 23 d).

Norma j)
Los Estados deben alentar la divulgación responsable de información sobre las vulnerabilidades relacionadas con las TIC y compartir la información conexa sobre los recursos disponibles ante tales vulnerabilidades a fin de limitar, y posiblemente eliminar, las amenazas potenciales para las TIC o las infraestructuras que dependen de ellas.

Medidas voluntarias y prácticas para aplicar la norma

Medidas nacionales

☐ 1. Establecer políticas y programas de divulgación de las vulnerabilidades, por ejemplo, un proceso coordinado de divulgación de vulnerabilidades para minimizar el daño que los productos vulnerables suponen para la sociedad y sistematizar la notificación de vulnerabilidades relacionadas con las TIC[51].

☐ 2. En consulta con el sector económico pertinente y otros actores de la seguridad de las TIC, desarrollar orientaciones e incentivos, en consonancia con las normas técnicas internacionales pertinentes, sobre:
- La notificación y gestión responsables de las vulnerabilidades y las funciones y responsabilidades respectivas de las distintas partes interesadas en los procesos de notificación;
- Los tipos de información técnica que deben divulgarse o compartirse públicamente, incluido el intercambio de información técnica sobre incidentes relacionados con las TIC que sean graves; y
- El modo de manejar los datos sensibles y garantizar la seguridad y confidencialidad de la información[52].

☐ 3. Establecer medidas que faciliten la cooperación internacional en materia de notificación responsable de vulnerabilidades relacionadas con las TIC y las solicitudes de asistencia entre los países y los equipos de respuesta de emergencia, en consonancia con la legislación nacional[53].

☐ 4. Establecer protecciones jurídicas para los investigadores y los expertos en pruebas de intrusión[54].

Medidas que requieren cooperación internacional

☐ 5. Establecer marcos jurídicos, políticas y programas imparciales, o participar en ellos, para orientar la toma de decisiones sobre el tratamiento de las vulnerabilidades relacionadas con las TIC y limitar su distribución comercial como medio de protección contra cualquier uso indebido[55].

☐ 6. Utilizar los organismos multilaterales, regionales y subregionales existentes y otros cauces y plataformas pertinentes en los que participen distintas partes interesadas para desarrollar una interpretación compartida de los mecanismos y procesos para la divulgación responsable de vulnerabilidades[56].

---

[51] A/76/135, párr. 61.
[52] A/76/135, párr. 63.
[53] A/76/135, párr. 61.
[54] A/76/135, párr. 62.
[55] A/76/135, párr. 62.
[56] A/76/135, párr. 64.

Norma k)
Los Estados no deben realizar ni apoyar a sabiendas actividades que perjudiquen los sistemas de información de los equipos de respuesta de emergencia autorizados (a veces conocidos como equipos de respuesta a emergencias informáticas o equipos de respuesta a incidentes de ciberseguridad) de otro Estado. Un Estado no debe utilizar los equipos autorizados de respuesta de emergencia para realizar actividades malintencionadas a nivel internacional.

Medidas voluntarias y prácticas para aplicar la norma

Medidas nacionales

☐ 1. Considerar la posibilidad de categorizar los EREI/ERISI como parte de las infraestructuras críticas nacionales[57].

☐ 2. Establecer un marco nacional de gestión de incidentes de seguridad de las TIC con funciones y responsabilidades específicas, incluso para los EREI/ERISI, para facilitar la cooperación y coordinación entre esos equipos y otros organismos técnicos y de seguridad pertinentes a nivel nacional, regional e internacional[58].

☐ 3. Incluir en el marco nacional de gestión de incidentes de seguridad de las TIC políticas, medidas reguladoras o procedimientos que aclaren el estatus, la autoridad y los mandatos de los EREI/ERISI y que distingan las funciones únicas de esos equipos de otras funciones gubernamentales[59].

☐ 4. Considerar la posibilidad de declarar públicamente o establecer medidas que afirmen que no utilizarán los equipos de respuesta de emergencia autorizados para realizar actividades internacionales malintencionadas, y reconocer y respetar los ámbitos de operación y los principios éticos que orientan la labor de los equipos de respuesta de emergencia autorizados[60].

Medidas que requieren cooperación internacional

☐ 5. Facilitar la cooperación y la coordinación entre los EREI/ERISI y otros organismos técnicos y de seguridad pertinentes a nivel nacional, regional e internacional, por medios como marcos nacionales de gestión de incidentes de seguridad de las TIC[61].

[57] A/76/135, párr. 66.
[58] A/76/135, párr. 68.
[59] A/76/135, párr. 68.
[60] A/76/135, párr. 67.
[61] A/76/135, párr. 68.

Anexo B

Lista inicial de medidas globales voluntarias de fomento de la confianza

A continuación figura una lista inicial, no exhaustiva, de medidas globales voluntarias de fomento de la confianza (MFC). Estas medidas globales de fomento de la confianza se han extraído del informe final de 2021 del grupo de trabajo de composición abierta y de los informes anuales primero y segundo sobre los progresos realizados por el grupo de trabajo. Con el tiempo podrán añadirse a esta lista otras medidas globales de fomento de la confianza, si procede, que reflejen los debates en el seno del grupo de trabajo.

MFC 1. Designar puntos de contacto nacionales para el Directorio Mundial de Puntos de Contacto y poner en funcionamiento y utilizar el Directorio Mundial de Puntos de Contacto

a) Los Estados acuerdan establecer, a partir del trabajo ya realizado a nivel regional, un directorio global e intergubernamental de puntos de contacto. Durante los períodos de sesiones cuarto y quinto del grupo de trabajo, los Estados entablan nuevos debates centrados en la elaboración de ese directorio, sobre la base de un consenso, y entablan debates también sobre las iniciativas conexas para la creación de capacidad, teniendo en cuenta las mejores prácticas disponibles, como las experiencias regionales y subregionales, cuando proceda.

[Primer informe anual sobre los progresos realizados por el grupo de trabajo, sección sobre las medidas de fomento de la confianza, próximas medidas recomendadas, párrafo 2]

b) Los Estados que aún no lo han hecho consideran la designación de un punto de contacto nacional en los planos técnico, diplomático y de políticas, teniendo en cuenta las capacidades diferenciadas. Se alienta también a los Estados a que sigan examinando las modalidades para establecer un directorio de esos puntos de contacto a nivel mundial.

[Informe del grupo de trabajo de 2021, párrafo 51]

c) Se alienta a los Estados a que pongan en funcionamiento y utilicen el Directorio Mundial de Puntos de Contacto llevando a cabo lo siguiente:

i) Comprobaciones de comunicación en forma de pruebas de *ping*;

ii) Intercambio voluntario de información, incluso en caso de incidente urgente o relevante relacionado con las TIC, facilitado a través del Directorio Mundial de Puntos de Contacto;

iii) Ejercicios de simulación de los aspectos prácticos de la participación en un Directorio Mundial de Puntos de Contacto;

iv) Reuniones voluntarias, periódicas y presenciales o virtuales de los puntos de contacto para compartir información práctica y experiencias sobre la puesta en funcionamiento y la utilización del Directorio Mundial de Puntos de Contacto;

v) Utilización del directorio de puntos de contacto para establecer la comunicación entre los puntos de contacto de acuerdo con las modalidades del Directorio Mundial de Puntos de Contacto.

MFC 2. Seguir intercambiando puntos de vista y emprendiendo diálogos y consultas bilaterales, subregionales, regionales, transregionales y multilaterales entre los Estados

a) Los Estados concluyeron que el diálogo dentro del grupo de trabajo de composición abierta era, en sí mismo, una medida de fomento de la confianza, ya que estimulaba un intercambio de opiniones abierto y transparente sobre las percepciones de las amenazas y las vulnerabilidades, el comportamiento responsable de los Estados y otros agentes y buenas prácticas, lo que en última instancia contribuía al desarrollo y la implementación colectivos del marco para el comportamiento responsable de los Estados en el uso de las TIC.

[Informe del grupo de trabajo de 2021 (A/75/816), párrafo 43]

b) Los Estados exploran mecanismos para mantener intercambios interregionales periódicos de lecciones aprendidas y buenas prácticas con respecto a las medidas de fomento de la confianza, teniendo en cuenta las diferencias en los contextos regionales y las estructuras de las organizaciones pertinentes.

[Informe del grupo de trabajo de 2021 (A/75/816), párrafo 52]

c) Los Estados siguen estudiando la posibilidad de adoptar medidas de fomento de la confianza a nivel bilateral, regional y multilateral y fomentan las oportunidades para el ejercicio cooperativo de esas medidas.

[Informe del grupo de trabajo de 2021, párrafo 53]

d) Los Estados siguieron destacando que el propio grupo de trabajo servía como medida de fomento de la confianza.

[Primer informe anual sobre los progresos realizados por el grupo de trabajo, párrafo 16 e)]

MFC 3. Compartir información, de forma voluntaria, como documentos conceptuales nacionales sobre las TIC, estrategias, políticas y programas nacionales, legislación y mejores prácticas

a) Los Estados siguen informando al Secretario General, de forma voluntaria, sobre sus opiniones y evaluaciones, incluyendo información adicional sobre las lecciones aprendidas y las buenas prácticas en relación con las medidas de fomento de la confianza pertinentes en los planos bilateral, regional o multilateral.

[Informe del grupo de trabajo de 2021, párrafo 48]

b) Los Estados aplican voluntariamente medidas de transparencia compartiendo información y lecciones pertinentes en el formato y los foros que eligen, según corresponda, en particular a través del Portal de Política Cibernética del Instituto de las Naciones Unidas de Investigación sobre el Desarme (UNIDIR).

[Informe del grupo de trabajo de 2021, párrafo 50]

c) Se alienta a los Estados a que sigan compartiendo, de forma voluntaria, documentos conceptuales, estrategias, políticas y programas nacionales, así como información sobre las instituciones y estructuras de las TIC con relevancia para la seguridad internacional, incluso a través del informe del Secretario General sobre los avances en el ámbito de las tecnologías de la información y la comunicación en el contexto de la seguridad internacional, así como del Portal de Política Cibernética del UNIDIR, según proceda.

[Primer informe anual sobre los progresos realizados por el grupo de trabajo, sección sobre las medidas de fomento de la confianza, próximas medidas recomendadas, párrafo 5]

MFC 4. Fomentar oportunidades para el desarrollo y el ejercicio cooperativos de las medidas de fomento de la confianza

a) Los Estados determinan y examinan voluntariamente las medidas de fomento de la confianza adecuadas para sus contextos específicos y cooperan con otros Estados en su implementación.

[Informe del grupo de trabajo de 2021, párrafo 49]

b) Los Estados siguen estudiando la posibilidad de adoptar medidas de fomento de la confianza a nivel bilateral, regional y multilateral y fomentan las oportunidades para el ejercicio cooperativo de esas medidas.

[Informe del grupo de trabajo de 2021, párrafo 53]

c) Los Estados siguen intercambiando puntos de vista en el grupo de trabajo a propósito del desarrollo y la aplicación de medidas de fomento de la confianza, incluido el posible desarrollo de medidas de fomento de la confianza adicionales.

[Primer informe anual sobre los progresos realizados por el grupo de trabajo, sección sobre las medidas de fomento de la confianza, próximas medidas recomendadas, párrafo 1]

Además de las medidas de fomento de la confianza globales ya enumeradas, los Estados han añadido las siguientes medidas globales voluntarias de fomento de la confianza:

MFC 5. Promover el intercambio de información sobre cooperación y alianzas entre Estados para reforzar la capacidad en materia de seguridad de las TIC y favorecer la aplicación activa de las medidas de fomento de la confianza

Los programas de creación de capacidad son un medio de colaboración importante que podría fortalecer las relaciones y fomentar la confianza entre los Estados.

MFC 6. Organizar de forma periódica seminarios, talleres y programas de capacitación sobre la seguridad de las TIC

Organizar de forma periódica seminarios, talleres y programas de capacitación sobre temas relevantes relacionados con la seguridad de las TIC, en los que los Estados estén representados de manera inclusiva, podría aumentar la comunicación y el entendimiento mutuo y contribuir al fomento de la confianza.

MFC 7. Intercambiar información y mejores prácticas sobre, entre otras cosas, la protección de las infraestructuras críticas y las infraestructuras críticas de información, por medios como crear la capacidad correspondiente

Intercambiar información y mejores prácticas sobre, entre otras cosas, la protección de las infraestructuras críticas y las infraestructuras críticas de información, por medios como crear la capacidad correspondiente, podría fomentar la confianza entre los Estados.

MFC 8. Reforzar las alianzas y la cooperación público-privadas en materia de seguridad de las TIC

Para detectar incidentes relacionados con las TIC, darles respuesta y defenderse y recuperarse de ellos se requieren diversas capacidades y conocimientos técnicos. A ese respecto, las alianzas y la cooperación público-privadas, en particular el diálogo periódico y el intercambio de buenas prácticas, podrían contribuir a fomentar la confianza.

Anexo C

Elementos del mecanismo permanente de composición abierta y orientado a la acción sobre la seguridad de las TIC en el contexto de la seguridad internacional

1. En el presente documento se exponen los elementos para crear en las Naciones Unidas un futuro mecanismo permanente sobre la seguridad de las TIC en el contexto de la seguridad internacional cuando concluya la labor del grupo de trabajo de composición abierta sobre la seguridad de las TIC y de su uso (2021-2025). El mecanismo permanente será de composición abierta y estará orientado a la acción; cimentará su labor en los acuerdos consensuados sobre el marco de comportamiento responsable de los Estados en el uso de las TIC de anteriores informes del grupo de trabajo y del Grupo de Expertos Gubernamentales[1] con el objetivo de seguir promoviendo un entorno de TIC abierto, seguro, estable, accesible, pacífico e interoperable[2].

2. Partiendo de los objetivos enunciados en las resoluciones pertinentes de la Asamblea General, incluidas, entre otras, las resoluciones 78/16 y 78/237, en relación con los debates sobre el diálogo institucional periódico celebrados en el seno del grupo de trabajo, los Estados recomendaron que el futuro mecanismo permanente se estableciera en consonancia con los elementos de consenso contenidos en el presente documento con el fin de que la transición al nuevo mecanismo fuera fluida.

Principios rectores

3. La creación del futuro mecanismo permanente se guiará por los elementos recomendados por consenso en el grupo de trabajo, en particular los elementos comunes recomendados por consenso en los párrafos 55 a 57 del segundo informe anual sobre los progresos realizados por el grupo de trabajo, los cuales se reproducen a continuación.

4. El futuro mecanismo permanente se basará en los siguientes elementos comunes:

a) Se tratará de un mecanismo permanente de una sola vía, dirigido por los Estados y bajo los auspicios de las Naciones Unidas, que dependerá de la Primera Comisión de la Asamblea General de las Naciones Unidas;

b) El objetivo del futuro mecanismo será seguir promoviendo un entorno de TIC abierto, seguro, estable, accesible, pacífico e interoperable;

c) El futuro mecanismo tomará como base de su labor los acuerdos consensuados sobre el marco de comportamiento responsable de los Estados en el uso de las TIC de anteriores informes del grupo de trabajo y del Grupo de Expertos Gubernamentales;

d) Se tratará de un proceso abierto, inclusivo, transparente, sostenible y flexible, capaz de evolucionar en función de las necesidades de los Estados y de la evolución del entorno de las TIC.

5. Los Estados reconocieron la importancia del principio de consenso, en lo tocante tanto al establecimiento del futuro mecanismo como a sus procesos de toma de decisiones.

[1] Segundo informe anual sobre los progresos realizados, párr. 55 c).
[2] Segundo informe anual sobre los progresos realizados, párr. 55 b).

6. Otras partes interesadas, como las empresas, las organizaciones no gubernamentales y los círculos académicos, podrán contribuir a un futuro diálogo institucional periódico, según proceda.

7. Los Estados reconocieron que las organizaciones regionales y subregionales podrían seguir desempeñando un papel importante en la aplicación del marco de comportamiento responsable de los Estados en el uso de las TIC. Además, los intercambios regionales, interregionales e interinstitucionales podían establecer nuevas vías de colaboración, cooperación y aprendizaje mutuo. Dado que no todos los Estados eran miembros de una organización regional y no todas las organizaciones regionales se centraban en la cuestión de la seguridad en el uso de las TIC, los Estados señalaron que los esfuerzos regionales eran complementarios a la labor del futuro mecanismo permanente[3].

Funciones y alcance

8. El futuro mecanismo permanente se ocupará de la cuestión de la seguridad de las TIC en el contexto de la seguridad internacional con el objetivo de promover un entorno de TIC abierto, seguro, estable, accesible, pacífico e interoperable.

9. Además de velar por la continuidad de la labor del grupo de trabajo de composición abierta (2021-2025) y aprovechar sus resultados y los acuerdos anteriores del grupo de trabajo y el Grupo de Expertos Gubernamentales, las funciones del mecanismo permanente de composición abierta y orientado a la acción consisten en fortalecer la capacidad de todos los Estados en materia de seguridad de las TIC, en particular desarrollar y aplicar el marco acumulativo y evolutivo de comportamiento responsable de los Estados en el uso de las TIC, fomentar la aplicación de dicho marco y seguir desarrollándolo. Guiándose por las funciones ya enumeradas, el mecanismo permanente de composición abierta y orientado a la acción tratará, entre otras, las cuestiones siguientes facilitando debates integrados, orientados a las políticas y transversales: las amenazas actuales y potenciales, las normas voluntarias y no vinculantes de comportamiento responsable de los Estados y sus medios de aplicación, reconociendo que con el tiempo podrían formularse normas adicionales. El mecanismo permanente de composición abierta y orientado a la acción también se ocupará de seguir estudiando el modo en que el derecho internacional es aplicable al uso de las TIC, teniendo en cuenta la posibilidad de formular otras obligaciones vinculantes, si procede, y la posible existencia de lagunas respecto de esa aplicación, así como la formulación de otras obligaciones jurídicamente vinculantes adicionales[4], de diseñar y aplicar medidas de fomento de la confianza y de desarrollar y poner en práctica actividades de creación de capacidad.

10. Habida cuenta de las funciones del futuro mecanismo permanente, los Estados reconocieron que la cooperación y la asistencia internacionales podían ser esenciales para que los Estados pudieran proteger las TIC y velar por su uso pacífico[5]. Además, dado que la creación de capacidad es transversal a las cuestiones de seguridad de las TIC y actúa como catalizador que refuerza la resiliencia de las TIC y la capacidad de los Estados de detectar actividades malintencionadas relacionadas con las TIC, defenderse de ellas o darles respuesta, desarrollar enfoques de creación de capacidad orientados a la acción, como la correspondencia entre las necesidades y los recursos y la asistencia técnica, será una función importante del futuro mecanismo permanente. Además, los Estados reconocen que la creación de capacidad también es necesaria

[3] Primer informe anual sobre los progresos realizados (A/77/275), párr. 5, y segundo informe anual sobre los progresos realizados (A/78/265), párr. 7.
[4] Segundo informe anual sobre los progresos realizados, párr. 32.
[5] Informe del Grupo de Expertos Gubernamentales de 2015, párr. 19.

para que los Estados puedan participar en el futuro mecanismo permanente de forma inclusiva e igualitaria.

11. El futuro mecanismo permanente promoverá la colaboración y la cooperación con las partes interesadas, como las empresas, las organizaciones no gubernamentales y el mundo académico, aprendiendo de la experiencia del proceso del grupo de trabajo y basándose en ella. La participación de otras partes interesadas, como empresas, organizaciones no gubernamentales y el mundo académico, en el futuro mecanismo permanente atenderá a lo siguiente:

a) El objetivo de promover debates inclusivos en el futuro mecanismo permanente aprovechando los conocimientos especializados pertinentes para apoyar la labor del mecanismo, según proceda;

b) La inclusión de oportunidades de consulta entre los Estados y otras partes interesadas, como las empresas, las organizaciones no gubernamentales y el mundo académico, en las sesiones plenarias sustantivas, los grupos temáticos específicos, las reuniones específicas entre períodos de sesiones y las conferencias de examen;

c) El principio general de que el futuro mecanismo permanente es un proceso dirigido por los Estados en el que las negociaciones y las decisiones sobre la seguridad de las TIC siguen siendo prerrogativa de los Estados;

d) La recomendación de que los Estados prosigan los debates en el seno del actual grupo de trabajo y formulen recomendaciones en su informe final, que se aprobará en julio de 2025, acerca de las modalidades de participación de otras partes interesadas, como las empresas, las organizaciones no gubernamentales y el mundo académico, en el futuro mecanismo permanente.

Estructura

12. El futuro mecanismo permanente se estructurará en un ciclo quinquenal compuesto por dos ciclos bienales seguidos de un ciclo de examen de un año. El futuro mecanismo permanente celebrará las reuniones siguientes:

a) **Sesiones plenarias sustantivas.** Se celebrará una sesión plenaria sustantiva al año durante cada ciclo bienal, con una duración mínima de una semana. En las sesiones plenarias sustantivas se mantendrán debates de acuerdo con las funciones y el alcance establecidos anteriormente y se examinarán la labor y las recomendaciones de los grupos temáticos específicos;

b) **Grupos temáticos específicos.** El futuro mecanismo permanente adoptará decisiones para crear grupos temáticos específicos que mantendrán debates especializados, según sea necesario. Los grupos temáticos específicos suministrarán a las sesiones plenarias sustantivas información actualizada y recomendaciones. Los Estados seguirán debatiendo en el seno del actual grupo de trabajo los grupos temáticos específicos del futuro mecanismo permanente y presentarán recomendaciones en el informe final del grupo de trabajo, que se aprobará en julio de 2025;

c) **Reuniones específicas entre períodos de sesiones.** La Presidencia del futuro mecanismo permanente, en consulta con los Estados, también podrá convocar reuniones específicas entre períodos de sesiones para entablar debates adicionales sobre cuestiones específicas o para examinar informes y recomendaciones, según sea necesario;

d) **Conferencia de examen.** Se celebrará una conferencia de examen cada cinco años para examinar el funcionamiento efectivo del futuro mecanismo permanente y dar dirección estratégica y orientación a las sesiones plenarias

sustantivas y los grupos temáticos específicos de los cuatro años siguientes. Además, en la conferencia de examen los Estados también podrán decidir por consenso modificar los elementos del futuro mecanismo permanente que figuran en el presente documento.

13. En cada ciclo bienal, el futuro mecanismo permanente estará dirigido por una Presidencia elegida para un período de dos años teniendo en cuenta la representación geográfica equitativa. Se elegirá también, para un período de un año y teniendo en cuenta la representación geográfica equitativa, una Presidencia para dirigir el proceso de la conferencia de examen.

14. A fin de velar por su inclusividad, las reuniones del futuro mecanismo permanente, incluidas las sesiones plenarias sustantivas, las reuniones de cualquier grupo temático específico y las reuniones específicas entre períodos de sesiones, no se celebrarán en paralelo y podrán convocarse en formato híbrido.

Modalidades

15. El futuro mecanismo permanente funcionará como sigue:

a) El mecanismo permanente se establecerá como órgano subsidiario de la Asamblea General de las Naciones Unidas y dependerá de la Primera Comisión;

b) La Oficina de Asuntos de Desarme de las Naciones Unidas prestará servicios de secretaría al mecanismo permanente;

c) Se creará un portal electrónico o un sitio web para apoyar y facilitar la labor del mecanismo permanente;

d) El Directorio Mundial de Puntos de Contacto será una herramienta permanente voluntaria para uso de los Estados;

e) Las reuniones oficiales del mecanismo permanente tendrán lugar en la Sede de las Naciones Unidas (Nueva York).

16. Para que la transición de la labor del grupo de trabajo al futuro mecanismo permanente sea fluida, los Estados recomiendan las disposiciones siguientes:

a) Se celebrará un período de sesiones de organización a más tardar en marzo de 2026 para llevar a cabo, entre otras tareas: i) la elección de la Presidencia del futuro mecanismo permanente; ii) la aprobación del programa; iii) la creación de los grupos temáticos específicos; y iv) la adopción de otras modalidades, según sea necesario;

b) La primera sesión plenaria sustantiva tendrá lugar a más tardar en junio de 2026.

Adopción de decisiones

17. El futuro mecanismo permanente adoptará todas las decisiones atendiendo al principio de consenso. Partiendo de consultas con los Estados, la Presidencia podrá someter decisiones a la aprobación por consenso de los Estados en cualquier momento de una sesión plenaria sustantiva; las decisiones se formalizarán tan pronto como el futuro mecanismo permanente se pronuncie sobre ellas.