Naciones Unidas A/79/81

Asamblea General

Distr. general
21 de mayo de 2024
Español
Original: chino/español/francés/
inglés/ruso

**Septuagésimo noveno período de sesiones**
Tema 93 de la lista preliminar*
**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

## Informe del Secretario General

*Resumen*

El presente informe contiene un resumen consolidado de elementos de las comunicaciones presentadas por los Estados Miembros en cumplimiento de la resolución 78/237 de la Asamblea General, sin perjuicio de las posturas de cada uno de ellos. Consolida las opiniones de los Estados sobre la seguridad de las tecnologías de la información y las comunicaciones y su utilización, particularmente en relación con el futuro diálogo institucional periódico sobre estas cuestiones bajo los auspicios de las Naciones Unidas. Las opiniones recibidas de los Estados Miembros dentro del plazo comunicado se reflejan íntegramente en el anexo del presente informe. El informe concluye con las observaciones del Secretario General.

* A/79/50.



Se ruega reciclar

# Índice

# I. Introducción

1. En virtud del párrafo 8 de su resolución 78/237, la Asamblea General invitó a todos los Estados Miembros a que siguieran informando al Secretario General de sus opiniones y observaciones sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso, en particular sobre el futuro diálogo institucional periódico sobre esas cuestiones que se celebraría bajo los auspicios de las Naciones Unidas, y solicitó al Secretario General que en su septuagésimo octavo período de sesiones le presentase un informe en el que se recogieran dichas opiniones para que los Estados Miembros continuaran deliberando en las reuniones del octavo período 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), en 2024. El presente informe se ha preparado en cumplimiento de esa solicitud.

2. El 5 de enero de 2024, la Oficina de Asuntos de Desarme distribuyó una nota verbal a todos los Estados Miembros en la que señalaba a su atención el párrafo 8 de la resolución 78/237 y recababa sus opiniones al respecto. Las opiniones recibidas al 1 de mayo de 2024 se reproducen en el anexo del presente informe. Las opiniones recibidas después de esa fecha se han publicado en el portal Meetings Place de la Oficina de Asuntos de Desarme[1].

3. La sección II del presente informe recoge los antecedentes relacionados con los debates de los Estados sobre la cuestión del diálogo institucional periódico sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso. La sección III contiene un resumen consolidado de elementos recibidos de los Estados Miembros, sin perjuicio de las posturas de cada uno de ellos. En la sección IV se recogen las observaciones y conclusiones del Secretario General.

# II. Antecedentes

4. Bajo los auspicios 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), los Estados siguen debatiendo, de conformidad con el programa acordado del grupo de trabajo que figura en el documento A/AC.292/2021/1, la cuestión del establecimiento, bajo los auspicios de las Naciones Unidas, de un diálogo institucional periódico sobre cuestiones conexas, con amplia participación de los Estados. En el transcurso de siete períodos de sesiones sustantivos del grupo de trabajo, desde diciembre de 2021 hasta marzo de 2024, los Estados participaron en debates específicos para seguir discutiendo las propuestas sobre el diálogo institucional periódico, incluida la propuesta de un programa de acción.

5. A través del segundo informe anual sobre la marcha de los trabajos del grupo de trabajo, adoptado por consenso en julio de 2023 (A/78/265), los Estados convinieron seguir debatiendo sobre elementos adicionales y acordaron, en principio, que el futuro mecanismo de diálogo institucional periódico se basaría en los siguientes elementos comunes:

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

b) El objetivo del futuro mecanismo sería seguir promoviendo un entorno de tecnología de la información y las comunicaciones abierto, seguro, estable, accesible, pacífico e interoperable;

[1] https://meetings.unoda.org/ga-c1/general-assembly-first-committee-seventy-ninth-session-2024.

c) El futuro mecanismo tomaría como base de su trabajo los acuerdos consensuados sobre el marco de comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones de anteriores informes del grupo de trabajo de composición abierta y el Grupo de Expertos Gubernamentales;

d) Se trataría 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 la tecnología de la información y las comunicaciones.

6. Los Estados recalcaron además la importancia del principio de consenso, tanto en lo que respecta al establecimiento del futuro mecanismo en sí como a su proceso de adopción de decisiones. Además, se alentó a los Estados que estuvieran en condiciones de hacerlo a que consideraran la posibilidad de establecer o apoyar programas de patrocinio y otros mecanismos para garantizar una participación amplia en los procesos pertinentes de las Naciones Unidas.

7. En los debates del grupo de trabajo de composición abierta sobre un futuro diálogo institucional periódico sobre cuestiones relacionadas con la seguridad de la tecnología de la información y las comunicaciones, los Estados reflexionaron sobre los posibles objetivos y ámbito, estructura, modalidades, en particular para la toma de decisiones, y seguimiento de la aplicación. Para facilitar los debates, la Presidencia del grupo de trabajo de composición abierta presentó en febrero de 2024 un documento de debate sobre un proyecto de elementos para un mecanismo permanente de seguridad de la tecnología de la información y las comunicaciones, seguido de una versión revisada en mayo de 2024. También se solicitaron dos reuniones entre períodos de sesiones dedicadas al tema del diálogo institucional periódico a través del segundo informe anual sobre los progresos realizados. En esas sesiones, los Estados también entablarían debates centrados en la relación entre el programa de acción para promover el comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional y el grupo de trabajo de composición abierta[2].

# III. Opiniones relativas al diálogo institucional periódico sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso

*Ideas y principios generales*

8. En sus comunicaciones, varios Estados destacaron la amenaza de las actividades malintencionadas en el uso de las tecnologías de la información y las comunicaciones (TIC) y señalaron la creciente preocupación internacional por las posibles amenazas a la seguridad y la estabilidad internacionales. Se expresó preocupación por el desarrollo excesivo, por parte de algunos Estados, de capacidades en materia de TIC con fines incompatibles con el derecho internacional y con los objetivos de mantenimiento de la estabilidad y la seguridad internacionales. Se observó que algunos agentes habían infringido el derecho internacional mediante actividades relacionadas con las TIC. También se expresó preocupación por el efecto de las actividades malintencionadas en la seguridad y el bienestar de las personas.

9. Algunos Estados señalaron que las TIC podían ser un catalizador del progreso y el desarrollo humanos, aunque también se observó que dichas tecnologías podían utilizarse con fines incompatibles con el objetivo de mantener la seguridad

[2] Véase A/78/76.

internacional y de una forma que afectara negativamente al desarrollo económico y social.

10. Muchos Estados subrayaron que, a la luz de las actuales condiciones de seguridad, era necesario que el futuro diálogo institucional periódico sobre la seguridad de las TIC y de su uso se centrara en seguir fomentando un entorno abierto, seguro, estable, accesible y pacífico de tecnología de la información y las comunicaciones. Algunos Estados subrayaron también la importancia de la cooperación internacional entre Estados para mantener la estabilidad internacional en este ámbito.

11. Muchos Estados señalaron que cada vez era mayor la demanda de un mecanismo permanente de toma de decisiones sobre asuntos conexos bajo los auspicios de las Naciones Unidas. Además, muchos Estados también subrayaron la importancia de basarse en los acuerdos alcanzados en procesos anteriores bajo los auspicios de las Naciones Unidas, incluidos los Grupos de Expertos Gubernamentales y el Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional[3]. Algunos Estados destacaron la necesidad de basarse en ese "acervo colectivo", y observaron que estaba compuesto por las normas vigentes de uso responsable de las TIC por parte de los Estados, la aplicabilidad del derecho internacional al uso de esas tecnologías por parte de los Estados, las medidas de fomento de la confianza y la creación de capacidad. También se expresó la opinión de que el futuro mecanismo debería crear un espacio para debates más profundos sobre la aplicación práctica de los acuerdos alcanzados previamente. A este respecto, también se expresó la opinión de que el directorio intergubernamental de puntos de contacto debía ser un componente integral de un futuro mecanismo.

12. Varios Estados subrayaron la importancia de la continuidad en cuanto a los resultados consensuados en procesos anteriores. De manera similar, distintos Estados observaron que el nuevo mecanismo o plataforma institucional debía establecerse una vez concluido el mandato del actual grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025). Algunos Estados subrayaron que esto debería ocurrir a más tardar en 2026 para garantizar la continuidad.

13. Varios Estados recalcaron la importancia de evitar la duplicación de esfuerzos internacionales en este ámbito y advirtieron contra la búsqueda de procesos paralelos, haciendo referencia a problemas conexos de capacidad para las delegaciones. Numerosos Estados destacaron la importancia de un diálogo institucional periódico, permanente, inclusivo y de una sola vía, bajo los auspicios de las Naciones Unidas. Algunos Estados señalaron que el establecimiento de un mecanismo único, inclusivo y permanente también contribuiría a la previsibilidad y la estabilidad institucional, al tiempo que evitaría la necesidad de negociar nuevos mandatos a intervalos regulares. También se señaló que los Estados pequeños y en desarrollo con recursos limitados no podrían participar de forma sostenible en procesos paralelos de doble vía. Además, se expresó la opinión de que el futuro mecanismo debía servir de ventanilla única general para abordar la seguridad de las TIC.

14. Algunos Estados afirmaron 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 en el entorno de las TIC. A este respecto, se expresó la opinión de que en el futuro mecanismo se podría debatir más a fondo cómo se aplica el derecho internacional. Se propuso que en un futuro mecanismo se estudiara la posibilidad de crear una línea de trabajo específica sobre este tema. Se expresó la opinión de que un

[3] Véanse A/65/201, A/68/98, A/70/174, A/75/816 y A/76/135.

futuro mecanismo podría servir de marco integrador para los debates sobre derecho internacional, entre otras cosas para compartir opiniones nacionales, convocar reuniones informativas de expertos y estudiar actividades de creación de capacidad en ese ámbito.

15. Los Estados reflexionaron sobre diversos principios fundamentales que debían sustentar un futuro mecanismo de diálogo institucional periódico sobre la seguridad de las TIC y de su uso, entre ellos la apertura, la inclusividad y la transparencia, y que dicho mecanismo debería estar orientado a la acción, ser de una sola vía y tener carácter democrático. Se expresó la opinión de que el futuro mecanismo debía estar dirigido por los Estados y basarse en el cumplimiento de los principios de la Carta, como la igualdad soberana de los Estados, el no uso o amenaza de uso de la fuerza y el arreglo pacífico de controversias. También se propuso que incorporara una flexibilidad suficiente y un desarrollo evolutivo en consonancia con las necesidades cambiantes de los Estados y la aparición de nuevas tareas en el ámbito de la garantía de la seguridad en el uso de las TIC.

16. Varios Estados se refirieron a la propuesta de un programa de acción para promover el comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional. Se señaló que esta propuesta se había reflejado en informes anteriores de órganos conexos de las Naciones Unidas, incluidos los informes anuales consensuados del grupo de trabajo de composición abierta. También se señaló que la propuesta había sido apoyada por un grupo interregional de Estados y que podría servir de estructura permanente para los debates sobre las TIC en el contexto de la seguridad internacional, establecida tras concluir la labor del actual grupo de trabajo de composición abierta.

17. Varios Estados señalaron que debía crearse un grupo de trabajo permanente de composición abierta inmediatamente después de que concluyera la labor del actual, cuyo mandato termina en 2025. Dichos Estados observaron que el actual grupo de trabajo de composición abierta había demostrado su eficacia y pertinencia como el formato más adecuado para dicho mecanismo y para un grupo de trabajo permanente de composición abierta encargado de adoptar decisiones con el mandato de centrarse en seguir fomentando un entorno abierto, seguro, estable, accesible y pacífico de tecnología de la información y las comunicaciones mediante, entre otras cosas, la elaboración de reglas, normas y principios jurídicamente vinculantes de comportamiento responsable de los Estados y la creación de un mecanismo eficaz para su aplicación, como elementos de un futuro tratado universal para garantizar la seguridad de la información internacional.

*Ámbito y objetivos*

18. Muchos Estados subrayaron que el objetivo primordial de un futuro diálogo institucional periódico sobre la seguridad de las TIC y de su uso era contribuir a la paz y la seguridad internacionales en ese ámbito. Varios Estados subrayaron que el futuro mecanismo debía promover un entorno abierto, seguro, estable, accesible y pacífico con respecto a las TIC. Algunos Estados también señalaron que el futuro mecanismo debería facilitar el diálogo y la cooperación entre los Estados y contribuir a la prevención de conflictos y malentendidos.

19. Varios Estados subrayaron que las recomendaciones por consenso de los anteriores procesos de las Naciones Unidas, que dieron lugar a un marco consolidado de comportamiento responsable de los Estados en el uso de las TIC, debían seguir siendo el eje central de un futuro mecanismo institucional. Algunos Estados destacaron la importancia de apoyar la aplicación de los resultados previamente acordados, mientras que otros señalaron que el futuro mecanismo debía considerar la

aplicación práctica de los acuerdos alcanzados por el grupo de trabajo de composición abierta. Se propuso que el futuro mecanismo elaborase orientaciones concretas para ayudar a los Estados a aplicar el marco normativo acordado, así como a mejorar la comprensión del propio marco.

20. En sus comunicaciones, los Estados reflexionaron sobre la necesidad de seguir desarrollando el marco existente. Algunos Estados señalaron opciones para detectar posibles deficiencias, elaborar normas adicionales o formular nuevas reglas y obligaciones jurídicamente vinculantes. Varios Estados apoyaron la búsqueda de un instrumento jurídicamente vinculante, mientras que otros subrayaron que el marco podía seguir desarrollándose y actualizándose, si fuera necesario, en respuesta a las nuevas amenazas que fueran surgiendo con el tiempo. Distintos Estados señalaron que el mecanismo debía encontrar un equilibrio entre dos aspectos del trabajo igualmente importantes: la aplicación del marco establecido y su desarrollo ulterior.

21. Se expresó la opinión de que un futuro mecanismo debería mirar hacia delante y hacia atrás para centrarse tanto en la observación como en la aplicación del marco acordado existente de comportamiento responsable de los Estados en el uso de las TIC, en particular el enriquecimiento de la creación de capacidades, y la formulación de nuevas normas en respuesta a los últimos avances, por ejemplo sobre la seguridad de los datos, y la elaboración de nuevos planes de acción sobre creación de capacidades y de un instrumento jurídicamente vinculante.

22. Muchos Estados insistieron en que el tema de la creación de capacidad debía ocupar un lugar central en un futuro mecanismo. Algunos Estados subrayaron la importancia de aunar las iniciativas existentes, incluidas las iniciativas conexas de la Unión Internacional de Telecomunicaciones y el Banco Mundial. Se hizo referencia a los principios acordados de creación de capacidad anexos al segundo informe anual sobre la marcha de los trabajos 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)[4]. Varios Estados señalaron que un futuro mecanismo debería facilitar los esfuerzos de creación de capacidad, en particular mediante el intercambio de información sobre las mejores prácticas. Algunos Estados subrayaron la importancia de las iniciativas específicas y basadas en las necesidades. Se expresó la opinión de que la función de creación de capacidad del mecanismo debía estar directamente vinculada a los esfuerzos de los Estados a nivel nacional para aplicar el marco normativo de comportamiento responsable de los Estados.

23. También se planteó la posibilidad de crear un mecanismo de financiación específico, basado en la experiencia de los mecanismos existentes en otros foros de las Naciones Unidas, para apoyar los esfuerzos de creación de capacidad. Se propuso crear un “sistema de alianzas” voluntario e interregional, mediante el cual Estados con distintas capacidades podrían emparejarse para mejorar la cooperación e intercambiar buenas prácticas. Se propuso un mecanismo multicomponente de creación de capacidad, que incluiría intercambios sobre el panorama de las amenazas, la autoidentificación de las necesidades de capacidades y la adecuación de las necesidades a los recursos, así como un “bucle de retroalimentación” para intercambios sobre experiencias relacionadas.

24. Varios Estados señalaron que el futuro mecanismo podría servir de marco institucional general para iniciativas y esfuerzos conexos en el ámbito de la seguridad de las TIC, incluido el directorio intergubernamental de puntos de contacto.

25. Distintos Estados señalaron otros posibles ámbitos de interés, como el desarrollo de un concepto común sobre cómo se aplica el derecho internacional al uso

[4] A/78/265, anexo C.

de las TIC y cómo podrían adaptarse las normas existentes a las características específicas de este ámbito. Se expresó la opinión de que un futuro mecanismo podría hacer avanzar los debates sobre las amenazas existentes y emergentes y la forma en que el derecho internacional, incluido el derecho internacional humanitario y de los derechos humanos, se aplica al uso de las TIC por parte de los Estados. El desarrollo y la aplicación de medidas de fomento de la confianza y mecanismos de cooperación práctica entre los Estados también se señalaron como puntos a tratar.

*Establecimiento, modalidades y adopción de decisiones*

26. Los Estados reflexionaron de forma diversa sobre las modalidades de creación de un futuro mecanismo, así como sobre los esfuerzos preparatorios previos a su establecimiento. Se expresó la opinión de que las contribuciones presentadas por los Estados Miembros en el marco del actual grupo de trabajo de composición abierta, incluidas las relativas a la propuesta de programa de acción, el informe del Secretario General sobre dicho programa de acción, preparado de conformidad con la resolución 77/37 de la Asamblea General[5], el presente informe y las recomendaciones pertinentes contenidas en los informes del actual grupo de trabajo de composición abierta debían constituir la base para el establecimiento del futuro mecanismo en cuanto a su ámbito, estructura y modalidades.

27. Muchos Estados subrayaron la importancia de alcanzar un consenso sobre el ámbito, la estructura y las modalidades del futuro mecanismo. Muchos Estados se mostraron partidarios de seguir elaborando y desarrollando el mecanismo dentro del actual grupo de trabajo de composición abierta. Varios Estados apoyaron la celebración de nuevos debates específicos en el actual grupo de trabajo de composición abierta para desarrollar el mecanismo y buscar un consenso sobre su formato y estructura. En cuanto al programa de acción, varios Estados apoyaron la celebración de reuniones específicas entre períodos de sesiones sobre esa propuesta en 2024 y 2025 para desarrollar otros aspectos del mecanismo. También se propusieron nuevos debates sobre las consecuencias presupuestarias.

28. Se señaló la posibilidad de establecer un futuro diálogo institucional periódico mediante una resolución consensuada de la Asamblea General. A este respecto, se expresó la opinión de que una resolución de la Asamblea debería establecer un grupo de trabajo permanente de composición abierta. También se expresó la opinión de que el actual grupo de trabajo de composición abierta podía establecer el futuro mecanismo a través de una declaración política que posteriormente aprobaría la Asamblea General. Se indicó que afirmar el compromiso de los Estados de guiarse por el marco de comportamiento responsable de los Estados podía constituir un elemento clave de dicha declaración política.

29. En cuanto a la propuesta concreta de un programa de acción, varios Estados apoyaron su creación mediante una declaración política. Se indicó que la declaración debía completarse con una resolución de la Primera Comisión en la que se describiesen las tareas, la estructura y las modalidades del programa de acción. También se propuso la convocatoria de una conferencia internacional que se celebraría a más tardar en 2026 para elaborar y adoptar dicha declaración. Se expresó la opinión de que, en caso de que el actual grupo de trabajo de composición abierta no llegara a un consenso sobre un informe final, incluido un acuerdo sobre un mecanismo, sería necesaria una conferencia internacional más amplia u otro proceso preparatorio establecido a través de la Asamblea General para garantizar la continuidad de estos importantes debates multilaterales.

[5] A/78/76.

*Mecanismo de seguimiento y aplicación*

30. Los Estados formularon varias propuestas para el mecanismo de seguimiento, incluidas reuniones periódicas, como sesiones plenarias y conferencias de examen, así como reuniones entre períodos de sesiones, en particular de grupos de trabajo técnicos. También se propusieron reuniones oficiales anuales del mecanismo. Las propuestas sobre la frecuencia de las sesiones plenarias variaron de cada dos a cada tres años. Se expresó la opinión de que el futuro mecanismo debía convocar reuniones bienales para aplicar su programa de trabajo acordado. También se expresó la opinión de que sería útil examinar periódicamente las operaciones del mecanismo permanente para garantizar que sus enfoques fueran pertinentes para el dinámico panorama operativo de las amenazas.

31. Algunos Estados apoyaron la creación de grupos de trabajo técnicos que se centraran en cuestiones prioritarias específicas, como la aplicabilidad del derecho internacional y la elaboración de nuevas normas, reglas y principios, así como de obligaciones jurídicamente vinculantes, según procediese. Se expresó la opinión de que los grupos de trabajo técnicos constituirían la esencia de un mecanismo orientado a la acción. Se propuso crear subgrupos subsidiarios para estudiar aspectos concretos del mandato del mecanismo. Se expresó la opinión de que las reuniones de los grupos de trabajo técnicos sobre cuestiones específicas entre períodos de sesiones debían celebrarse en un formato híbrido para facilitar la amplia participación de los Estados. Se observó que las reuniones de los subgrupos no debían celebrarse en paralelo para garantizar la plena participación de las delegaciones. Para facilitar una amplia participación de los Estados, se propuso un programa de becas.

32. Los Estados propusieron varias periodicidades para las posibles conferencias de examen, por ejemplo, cada tres, cuatro o seis años. Algunos Estados observaron que dichas conferencias de examen debían examinar el marco de comportamiento responsable de los Estados con vistas a su actualización, en caso necesario, y proporcionar una dirección estratégica para el trabajo del mecanismo. Se expresó la opinión de que las conferencias de examen debían considerar si debían elaborarse por consenso normas, reglas, principios u obligaciones vinculantes adicionales.

33. Muchos Estados abordaron la importancia de la toma de decisiones por consenso en un futuro mecanismo. Algunos Estados subrayaron que las decisiones sobre cuestiones de fondo debían tomarse por consenso. Varios Estados expresaron la opinión de que el principio de toma de decisiones por consenso exclusivamente por los Estados debía establecerse claramente en el documento por el que se creara el futuro mecanismo. Los Estados propusieron diversas formas de consolidar las decisiones de los Estados en un futuro mecanismo, como informes bienales a la Asamblea General sobre los progresos realizados e informes anuales de procedimiento acompañados de las decisiones consensuadas pertinentes.

34. Algunos Estados señalaron la posibilidad de presentar informes nacionales voluntarios en el marco de un futuro mecanismo. Se propuso informar sobre la aplicación nacional del marco normativo, así como sobre las prácticas nacionales. Se propuso usar las herramientas existentes, como la encuesta nacional de aplicación de las recomendaciones de las Naciones Unidas sobre el uso responsable de las TIC por parte de los Estados en el contexto de la seguridad internacional y las Naciones Unidas[6].

35. Varios Estados señalaron que, si bien la toma de decisiones seguía siendo prerrogativa exclusiva de los Estados, la interacción con las organizaciones regionales y subregionales podía ser beneficiosa, entre otras cosas para aprovechar las sinergias

[6] https://nationalcybersurvey.cyberpolicyportal.org.

y basarse en las estructuras y plataformas de creación de capacidad existentes. Se propuso celebrar anualmente reuniones entre períodos de sesiones con representantes de dichas organizaciones, sobre la base de consultas con grupos de países y la Presidencia respectiva del futuro mecanismo. También se propuso poner en común las mejores prácticas en los planos internacional, interregional y regional.

36. Los Estados reflexionaron de diversas maneras sobre la participación de las entidades no gubernamentales en un futuro mecanismo, y pusieron como ejemplo las modalidades de participación en otros foros de las Naciones Unidas como el Comité Especial encargado de Elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos y el Grupo de Trabajo de Composición Abierta sobre el Envejecimiento. Muchos Estados señalaron que la participación de múltiples partes interesadas era importante para el futuro funcionamiento del mecanismo. Se observó que la participación inclusiva de las partes interesadas en el futuro diálogo institucional periódico sería decisiva para alcanzar el objetivo común de mantener la paz y la seguridad en el ámbito de las TIC y podría aportar valiosos conocimientos especializados sobre cuestiones como la evaluación de amenazas y la aplicación de normas. Algunos Estados apoyaron la participación de entidades no gubernamentales de acuerdo con las modalidades acordadas en el actual grupo de trabajo de composición abierta. Varios Estados apoyaron la participación oficial y las consultas periódicas con las partes interesadas, mientras que otros afirmaron que la colaboración con los agentes no estatales debía ser estrictamente consultiva e informal, por ejemplo, a través de reuniones anuales entre períodos de sesiones.

37. Algunos Estados señalaron que la Oficina de Asuntos de Desarme era la entidad apropiada para servir de secretaría de un futuro mecanismo.

# IV. Observaciones y conclusiones del Secretario General

38. Salvaguardar la paz y la seguridad en el ámbito de las tecnologías de la información y las comunicaciones sigue siendo una tarea urgente. Mientras crece la preocupación por el uso malintencionado de estas tecnologías por parte de diversos agentes, la comunidad internacional se enfrenta a una brecha digital cada vez mayor y a un plazo cada vez menor para alcanzar los Objetivos de Desarrollo Sostenible. Es imperativo adoptar medidas concretas para evitar que los conflictos se intensifiquen y se extiendan a este ámbito, lo cual incluye la protección de la vida humana frente a actividades malintencionadas.

39. Aunque la comunidad internacional se enfrenta a retos formidables para mantener la paz y la estabilidad en el ámbito de las tecnologías de la información y las comunicaciones, también existe una base sólida sobre la que construir. A lo largo de más de dos décadas, a través de procesos auspiciados por la Asamblea General, los Estados han logrado avances decisivos en la detección de las amenazas existentes y emergentes, y han desentrañado la aplicabilidad del derecho internacional al uso de las tecnologías de la información y las comunicaciones por parte de los Estados, han elaborado un marco de comportamiento responsable de los Estados en el uso de estas tecnologías y han considerado medidas de fomento de la confianza e iniciativas de creación de capacidad. Este progreso ha sido acumulativo y coherente, y se ha realizado sobre la base de acuerdos consensuados. Así pues, existe una base sólida para seguir avanzando.

40. Las iniciativas emprendidas por los Estados en el marco del actual grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025) son una prueba de que es posible emprender más actuaciones concretas en pos del objetivo común de un entorno

pacífico y seguro en el ámbito de las tecnologías de la información y las comunicaciones. Los avances constantes en este foro demuestran que, con la suficiente voluntad política, no solo pueden alcanzarse acuerdos comunes, sino que también pueden adoptarse medidas prácticas. A este respecto, acojo con satisfacción el acuerdo consensuado alcanzado por los Estados para establecer un directorio mundial e intergubernamental de puntos de contacto, con el fin de mejorar la interacción y la cooperación entre ellos. Se trata de un paso significativo que promueve la paz y la seguridad internacionales y aumenta la transparencia y la previsibilidad.

41. En este contexto, los Estados reconocieron la importancia fundamental de mantener un diálogo institucional periódico sobre estas cuestiones para contar con un margen suficiente que permita realizar progresos continuos. Estas cuestiones van a cobrar cada vez más importancia a medida que estas tecnologías se hagan omnipresentes y pasen a formar parte de nuestra vida cotidiana.

42. En general, los Estados están de acuerdo en que lo más adecuado es que este diálogo institucional periódico tenga lugar bajo los auspicios de las Naciones Unidas, que ofrecen una plataforma plenamente integradora para este tipo de debates. También existe la idea común de que dicho diálogo contribuye a los objetivos de reforzar la paz internacional, la estabilidad y la prevención de conflictos en el entorno de las tecnologías de la información y las comunicaciones. Los Estados también afirman varios principios fundamentales que sustentarían dicho diálogo, por ejemplo, la inclusividad, la transparencia y un enfoque orientado a la acción. Además, comparten la idea de que se necesita un mecanismo de vía única que facilite la más amplia participación de los Estados.

43. Sobre la base de estos amplios acuerdos y opiniones generalizadas, alcanzar un acuerdo consensuado acerca de un futuro diálogo institucional periódico sobre las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional parece una tarea alcanzable. A partir de los éxitos ya logrados, los Estados tienen una gran oportunidad en el actual grupo de trabajo de composición abierta para llegar a acuerdos sobre un mecanismo permanente de vía única bajo los auspicios de las Naciones Unidas que funcione de manera abierta, inclusiva y transparente. Los elementos comunes del futuro diálogo institucional periódico convenidos por consenso en el informe anual de 2023 sobre la marcha de los trabajos del grupo de trabajo de composición abierta constituyen un punto de partida lógico y útil. Estos asuntos son demasiado importantes para no aprovechar esta oportunidad de fomentar la confianza. Un mecanismo permanente bajo los auspicios de las Naciones Unidas representa la siguiente fase lógica de la consideración multilateral de estos asuntos, aprovechando los éxitos del pasado y sentando las bases para futuros avances.

# Anexo

## Respuestas recibidas de los Gobiernos

### Alemania

[Original: inglés
30 de abril de 2024]

#### A. Principios subyacentes del programa de acción

Alemania defiende el establecimiento de un programa de acción como foro orientado a la acción, permanente, transparente, flexible e inclusivo para entablar un diálogo institucional periódico sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso en el marco de la Primera Comisión. El programa de acción debería ser el mecanismo de seguimiento de una sola vía del actual grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025). Debería entrar en funcionamiento a más tardar en 2026 para aplicar los resultados del grupo de trabajo tras la conclusión de su mandato, reiterando la decisión contenida en la resolución 78/16 de la Asamblea General de establecer un mecanismo bajo los auspicios de las Naciones Unidas, con los objetivos específicos reafirmados en la resolución 78/37 y con los elementos comunes acordados por consenso en el segundo informe anual del grupo de trabajo de composición abierta (2021-2025) (A/78/265).

Deben evitarse los procesos paralelos o las dobles estructuras para no sobrecargar la capacidad de los Estados de participar de forma significativa y garantizar debates orientados a la acción. Para preparar una transición fluida, es necesario que los Estados sigan debatiendo en el actual grupo de trabajo de composición abierta sobre el alcance, la estructura y el contenido del programa de acción, con la ambición de alcanzar un consenso sobre el contenido y las modalidades del programa de acción. El objetivo debe ser que todos los Estados Miembros aprueben dicho programa de acción en una conferencia específica que se celebrará coincidiendo con el último período de sesiones del grupo de trabajo en 2025.

El propósito general del programa de acción es contribuir a la paz y la seguridad internacionales en el ciberespacio facilitando el diálogo y la cooperación entre los Estados en relación con la aplicación del marco internacional existente de comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones (TIC). Para ello, se necesita lo siguiente:

- La creación de cibercapacidad de conformidad con las directrices acordadas en el informe final de 2021 del grupo de trabajo de composición abierta sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional, y con los principios acordados de creación de capacidad confirmados en el anexo C del segundo informe anual sobre los progresos realizados. Aprovechar las sinergias con mecanismos de otros foros será decisivo para evitar la duplicación de estructuras y la dispersión de los recursos.
- Medidas de fomento de la confianza, incluida la aplicación efectiva de la lista inicial no exhaustiva de medidas de fomento de la confianza acordada en el segundo informe anual sobre los progresos realizados (A/78/265, anexo B), en particular el directorio mundial de puntos de contacto.
- Intercambio de mejores prácticas en los planos internacional, interregional y regional;
- La participación efectiva de las partes interesadas pertinentes.

Además, el programa de acción constituirá la plataforma permanente para avanzar en los debates sobre las amenazas existentes y emergentes, así como sobre la forma en que el derecho internacional, incluido el derecho internacional humanitario y los derechos humanos, se aplica al uso de las TIC por los Estados. Dentro del programa de acción, debe ser posible un mayor debate y, cuando corresponda, un desarrollo del marco internacional de comportamiento responsable de los Estados en el ciberespacio, con el fin de adaptarse y responder a las nuevas amenazas a medida que evolucionen con el tiempo.

El programa de acción debería proporcionar el marco institucional general para otros mecanismos de ciberseguridad que se están preparando actualmente en el grupo de trabajo, como un ciberportal, sugerido por la India, y un ciberrepositorio, sugerido por Kenya.

El objetivo general, los objetivos específicos y los principios subyacentes del programa de acción deberían consagrarse en una declaración política que deberá aprobar la Asamblea General. La declaración debería completarse con una resolución de la Primera Comisión en la que se describan las tareas, la estructura y las modalidades del programa de acción. Tanto la declaración política como la resolución de la Primera Comisión deberían basarse en el documento final de la conferencia específica que se celebrará en 2025, como se ha mencionado anteriormente.

## B. Tareas, estructura y modalidades del programa de acción

Teniendo en cuenta la experiencia adquirida con los instrumentos anteriores y existentes, las tareas del programa de acción deberían diseñarse de manera que se garantice la participación efectiva, inclusiva y transparente de los Estados y se permita medir los avances en la aplicación del marco de comportamiento responsable de los Estados, incluso mediante un mecanismo de presentación de informes voluntarios como la encuesta nacional sobre la implementación de las recomendaciones de las Naciones Unidas sobre el uso responsable de las TIC por los Estados en el contexto de la seguridad internacional del Instituto de las Naciones Unidas de Investigación sobre el Desarme (UNIDIR). La creación de capacidad y la cooperación, tanto entre los Estados como con las organizaciones regionales y los actores no estatales, son fundamentales para abordar las esferas en las que la aplicación nacional está retrasada.

Basándose en los elementos comunes acordados en el segundo informe anual consensuado sobre los progresos realizados, la estructura y las modalidades del programa de acción deben incluir:

a) Conferencias anuales, que se celebrarían en la Sede de las Naciones Unidas (Nueva York) con el fin de:

i) Examinar y medir los avances en la aplicación del marco y las tareas definidas;

ii) Debatir la posible evolución del marco, entre otras cosas avanzando en el entendimiento común de la aplicación del derecho internacional en el ciberespacio;

iii) Adoptar decisiones sobre temas específicos;

iv) Intercambiar información sobre las amenazas actuales y emergentes para la paz y la seguridad internacionales derivadas del uso de las TIC;

v) Profundizar en las medidas de creación de cibercapacidad;

vi) Estudiar la posible evolución del programa de acción de forma gradual, en función de las necesidades de los Estados Miembros, teniendo en cuenta los

cambios en el panorama de las amenazas y entendiendo que el programa de acción es un instrumento flexible;

b) La aplicación y posterior desarrollo de medidas de fomento de la confianza basadas en el directorio mundial de puntos de contacto que estableció el actual grupo de trabajo de composición abierta. Más allá de ser una medida de fomento de la confianza en sí misma, el directorio proporcionará la base para la aplicación de la lista mundial no exhaustiva de medidas de fomento de la confianza acordada en el segundo informe anual sobre los progresos realizados, con el objetivo general de reducir el riesgo de malentendidos y conflictos en el ciberespacio. También debe servir para debatir, adoptar y aplicar otras medidas mundiales de fomento de la confianza. Al facilitar la elaboración y aplicación de medidas específicas de fomento de la confianza, el directorio constituiría un pilar central del programa de acción, centrado en la aplicación del marco existente;

c) Conferencias de examen cada cuatro a seis años para permitir la posible adaptación del programa de acción a la evolución dinámica del ciberespacio y los riesgos conexos para la paz y la seguridad internacionales;

d) La Oficina de Asuntos de Desarme debería prestar servicios de secretaría para el programa de acción. Además de preparar las reuniones anuales y las conferencias de examen, la Oficina también se encargará de administrar el directorio mundial de puntos de contacto y otras medidas de fomento de la confianza;

e) El UNIDIR proporcionaría a los Estados los instrumentos de seguimiento y examen pertinentes (por ejemplo, listas de verificación de la aplicación de las normas, según lo acordado en el segundo informe anual consensuado sobre los progresos realizados) y llevaría a cabo actividades de investigación relacionadas con la aplicación del marco;

f) La posibilidad de celebrar reuniones adicionales de las líneas de trabajo técnicas en el período entre sesiones. Las líneas de trabajo técnicas específicas podrían centrarse, entre otras cosas, en temas como el fomento de la creación de cibercapacidad, las medidas de fomento de la confianza, la aplicación del derecho internacional (incluido el derecho internacional humanitario) y las amenazas actuales y emergentes. La participación en las líneas de trabajo debe ser voluntaria, abierta a todos los Estados y equilibrada desde el punto de vista regional. El número y la configuración de las líneas de trabajo, incluida la participación de las partes interesadas y la frecuencia de las reuniones y las posibles modalidades de trabajo híbridas, deben tener en cuenta las capacidades de los Estados para participar de forma significativa y deben decidirse por consenso en las reuniones anuales.

Los Estados mantendrán el derecho exclusivo de negociar los resultados y tomar decisiones dentro del programa de acción. Al mismo tiempo, el programa debe prever mecanismos de colaboración con las partes interesadas no gubernamentales (organizaciones multilaterales y regionales, sociedad civil, sector privado y mundo académico). El programa de acción debe ofrecer oportunidades para la participación inclusiva y significativa de las partes interesadas de manera similar a las modalidades del Comité Especial encargado de Elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos (en particular, cualquier veto de un Estado Miembro a la participación de una parte interesada debe justificarse públicamente; la exclusión de las partes interesadas se decidiría por votación). Ello incluye el derecho a intervenir y presentar aportaciones por escrito en las reuniones, las conferencias de examen y las reuniones adicionales de las líneas de trabajo técnicas durante el período entre sesiones. Además, para aumentar la inclusividad de las deliberaciones, deben ofrecerse opciones híbridas de participación para la mayoría de los formatos.

En particular, en el ámbito de las medidas de fomento de la confianza y la creación de capacidad, deberían aprovecharse las iniciativas y estructuras existentes a nivel regional y subregional o en otros foros y crearse sinergias (por ejemplo, con organizaciones regionales, el fondo fiduciario de donantes múltiples para la ciberseguridad del Banco Mundial y el Foro Mundial de Competencia Cibernética).

Los mecanismos de financiación existentes en otros foros de las Naciones Unidas, como el fondo Entidad Salvar Vidas o el Servicio Fiduciario de las Naciones Unidas de Apoyo a la Cooperación para la Regulación de los Armamentos en la esfera del control de armamentos, podrían proporcionar directrices útiles para establecer un mecanismo de apoyo a los esfuerzos de creación de cibercapacidad en forma de capacitación e intercambio de mejores prácticas. Además, podría preverse un programa de becas para facilitar una amplia representación de expertos de la capital de las delegaciones de los países en desarrollo.

Podría establecerse un "sistema de asociación" voluntario e interregional, en el que un Estado que disponga de capacidades elevadas con respecto a la aplicación del marco de comportamiento responsable de los Estados en el ciberespacio se empareje con uno o varios Estados con capacidades inferiores. Este mecanismo mejoraría la cooperación entre los Estados, facilitaría el diálogo y el intercambio de mejores prácticas y aumentaría las capacidades de los Estados para la aplicación general de las normas. El enfoque de "adoptar una medida de confianza" de la Organización para la Seguridad y la Cooperación en Europa podría servir de referencia a este respecto.

## Australia

[Original: inglés
1 de mayo de 2024]

Australia acoge con beneplácito la oportunidad, en respuesta a la invitación formulada en la resolución 78/237 de la Asamblea General, de exponer sus opiniones sobre la promoción de un comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional y fomentar el diálogo institucional periódico.

Esta presentación se basa en los escritos presentados por Australia en respuesta a las resoluciones 77/37 en 2023, 76/19 en 2022, 75/32 en 2021, 74/28 en 2020, 70/237 en 2016, 68/243 en 2014 y 65/41 en 2011 sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional.

### Estrategia de Ciberseguridad de Australia, 2023-2030

El 22 de noviembre de 2023, la Ministra de Ciberseguridad, Clare O'Neil, presentó la Estrategia de Ciberseguridad de Australia para 2023-2030, que establece el ideal de Australia para la ciberseguridad nacional e internacional a través de un planteamiento de escala nacional para impulsar la ciberresiliencia.

La Estrategia señaló seis escudos para construir ciberdefensas más sólidas y recuperarse rápidamente tras un ciberincidente: a) empresas y ciudadanos fuertes; b) tecnología segura; c) intercambio y bloqueo de amenazas de primer orden; d) protección de la infraestructura crítica; e) capacidades soberanas; y f) un liderazgo regional y mundial resiliente.

La Estrategia establece la determinación continua de Australia de dar forma, mantener y defender las reglas, normas y estándares cibernéticos internacionales, incluida la defensa del derecho internacional y las normas de comportamiento

responsable de los Estados en el ciberespacio, y el despliegue de todo el poder del Estado para disuadir a los agentes malintencionados y darles respuesta.

**Defender el derecho internacional y las normas de comportamiento responsable de los Estados en el ciberespacio**

Australia colaborará con sus actuales aliados y creará nuevas alianzas para defender el derecho internacional y el marco acordado de comportamiento responsable de los Estados que sustenta nuestra estabilidad, prosperidad, independencia y soberanía en el ciberespacio.

Todos los países han acordado un ciberespacio basado en normas, sustentado en el derecho y las normas internacionales vigentes. El derecho internacional, unido a las normas voluntarias acordadas sobre el comportamiento responsable de los Estados, las medidas de fomento de la confianza y la creación de capacidad, proporciona un marco sólido para la previsibilidad y la estabilidad en el ciberespacio. Si se aplica y se respeta, este marco proporciona un conjunto de herramientas para hacer frente a las amenazas que plantea la ciberactividad malintencionada generada y patrocinada por el Estado.

Australia colaborará con sus asociados internacionales en los debates de las Naciones Unidas para aclarar cómo se aplica el derecho internacional en el ciberespacio y reforzar la aplicación del marco de comportamiento responsable de los Estados en el ciberespacio. Dichos esfuerzos incluirán la mejora de la cooperación a través de foros regionales, por ejemplo, en el contexto del Foro de las Islas del Pacífico y mediante la colaboración con el Foro Regional de la Asociación de Naciones de Asia Sudoriental.

**Desplegar todo el poder del Estado para disuadir a los agentes malintencionados y darles respuesta**

Australia desplegará todo el poder del Estado para disuadir a los agentes malintencionados y darles respuesta. Australia colaborará con sus asociados internacionales para hacer que las personas y organizaciones que hagan que el ciberespacio sea menos seguro paguen un precio por ello. Ello supone denunciar los casos en los que los Estados actúan para socavar o infringir el derecho y las normas internacionales, e imponer sanciones a quienes lleven a cabo o faciliten ciberincidentes importantes (cuando tengamos pruebas suficientes y redunde en nuestro interés nacional hacerlo).

En todas sus acciones, Australia respetará el derecho internacional vigente y las normas voluntarias acordadas sobre el comportamiento responsable de los Estados en el ciberespacio.

**Contribuir a una región ciberresiliente**

Australia seguirá colaborando con sus vecinos del Pacífico y Asia Sudoriental para construir una región más ciberresiliente. La Embajada de Australia para Asuntos Cibernéticos y Tecnología Crítica seguirá coordinando nuestra cooperación y asistencia.

Australia está reorientando sus iniciativas de cooperación y creación de capacidad en materia cibernética para que sean más específicas, eficaces y sostenibles, y para que nuestros vecinos puedan prevenir mejor los ciberincidentes y recuperarse rápidamente cuando se produzcan. Reconociendo que la población se implica en los problemas de ciberseguridad de diferentes maneras, nuestros esfuerzos seguirán teniendo en cuenta la igualdad de género, la discapacidad y la inclusión social. Ello abarca el apoyo continuo a la agenda de las Naciones Unidas sobre las

mujeres y la paz y la seguridad, así como al Plan de Acción Nacional de Australia sobre las Mujeres, la Paz y la Seguridad para 2021-2031.

Cuando se produzcan ciberincidentes graves en nuestra región, Australia estará en mejor posición de responder a las solicitudes de ayuda. Australia está creando un equipo regional de respuesta a las cibercrisis en el Departamento de Relaciones Exteriores y Comercio, sobre la base de la experiencia de la administración, la industria y la comunidad técnica. En respuesta a las peticiones de los gobiernos tras ciberincidentes importantes en la región, el equipo ayudará a frenar la propagación y el impacto de los ciberincidentes y a restablecer servicios e infraestructuras críticos.

**Diálogo institucional periódico**

**Programa de acción para promover el comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional**

Australia apoya la creación de un mecanismo único, permanente, flexible, inclusivo, transparente y orientado a la acción, bajo los auspicios de la Primera Comisión, para debatir, aplicar y hacer avanzar el marco de comportamiento responsable de los Estados en el ciberespacio, acordado y reafirmado por consenso por la Asamblea General. El marco engloba el derecho internacional, así como normas y medidas de fomento de la confianza, y se respalda con la coordinación de medidas de creación de capacidad. El programa de acción debería proporcionar un foro en el que los 193 Estados Miembros pudieran participar de forma significativa en el debate y en las medidas de acción, tanto de manera periódica como continuada. El programa de acción debería ser capaz de crecer, evolucionar y desarrollarse: debería apoyar la implementación del marco acordado existente y permitir su posible desarrollo posterior, por consenso, a medida que surjan nuevas amenazas y retos.

En su resolución 77/37, la Asamblea General acogió con satisfacción la propuesta de crear un programa de acción y solicitó al Secretario General que recabara la opinión de los Estados Miembros sobre el alcance, la estructura y el contenido del programa de acción. En ese informe (A/78/76) se recomendó que los Estados siguieran debatiendo el posible alcance, estructura, principios, contenido, funciones y mecanismo de seguimiento de la propuesta de programa de acción bajo los auspicios 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), basándose en las opiniones expresadas en el informe y teniendo en cuenta al mismo tiempo las consultas regionales y subregionales organizadas por la Oficina de Asuntos de Desarme de conformidad con lo previsto en la resolución 77/37 de la Asamblea General.

El grupo de trabajo de composición abierta desempeña una función clave en la elaboración y preparación del programa de acción. El programa de acción debe basarse en los logros alcanzados mediante un arduo trabajo de consenso y en los debates acumulativos de los seis últimos grupos de expertos gubernamentales y de los grupos de trabajo de composición abierta inicial y actual. Un mecanismo permanente representa la siguiente fase o evolución en la ciberarquitectura de las Naciones Unidas, que se basa en lo que ha habido antes y garantiza que estas cuestiones reciban la atención y la importancia que merecen en lo sucesivo.

En su resolución 78/16, la Asamblea General decidió crear, bajo los auspicios de las Naciones Unidas, una vez que concluyera la labor del grupo de trabajo de composición abierta (2021-2025) y a más tardar en 2026, un mecanismo permanente, inclusivo y orientado a la acción que tendría los objetivos específicos que se señalaban en su resolución 77/37 y los elementos comunes del futuro diálogo

institucional periódico convenidos por consenso en el informe anual del grupo de trabajo de composición abierta (2021-2025) sobre los progresos realizados presentado en 2023.

Australia apoya la propuesta de convocar una conferencia internacional en 2025 para aprobar el texto fundacional del programa de acción, sobre la base de los trabajos preparatorios llevados a cabo en el seno del grupo de trabajo de composición abierta (2021-2025).

Australia respalda un documento fundacional del programa de acción que establezca los compromisos de los Estados y proporcione un mecanismo que pueda ser aprobado por una resolución de la Asamblea General. El documento fundacional, que podría redactarse como una declaración política, debe:

- Respaldar y reafirmar el compromiso político de los Estados con el marco (incluida la aplicación del derecho internacional vigente en el ciberespacio), como se acordó en los informes de los grupos de expertos gubernamentales[1] y en el informe del grupo de trabajo de composición abierta[2].
- Recordar las amenazas existentes y emergentes para la seguridad internacional relacionadas con el uso malintencionado de las tecnologías de la información y las comunicaciones (TIC), basándose en las evaluaciones de las amenazas contenidas en los informes de los grupos de expertos gubernamentales y el grupo de trabajo de composición abierta.
- Establecer un mecanismo institucional permanente para promover la aplicación de este marco (incluido el apoyo a las capacidades de los Estados para hacerlo) y las modalidades pertinentes.
- Permitir un mayor desarrollo y actualizaciones del marco, según proceda, para incluir principios, recomendaciones y compromisos de consenso en caso de que la Asamblea General, por consenso, apruebe un informe del grupo de trabajo de composición abierta, el Grupo de Expertos Gubernamentales u otros procesos de las Naciones Unidas, o mediante un acuerdo consensuado en una conferencia de examen del programa de acción.
- Establecer áreas de trabajo prioritarias para el programa de acción basadas en cuestiones que la comunidad internacional acuerde debatir y abordar.
- Fomentar y alentar claramente la cooperación con los miembros pertinentes de la comunidad de múltiples partes interesadas en los ámbitos pertinentes.

En relación con el reglamento, Australia reitera que el programa de acción debería exigir que todas las cuestiones se acuerden por consenso (incluidos los informes, las recomendaciones y las declaraciones).

Para garantizar que las actividades del programa de acción se basen en pruebas y en datos, el programa de acción debería hacer hincapié en el apoyo a los esfuerzos de aplicación, incluso a través de actividades de creación de capacidad específicas, concretas y coordinadas. Las medidas para la creación de capacidad específica deberían elaborarse claramente dentro del programa de acción. Para promover una creación de capacidad específica, basada en las necesidades y fundamentada en una base empírica, el programa de acción podría animar a los Estados Miembros a que realizaran encuestas periódicas y autoevaluaciones sobre su aplicación del marco (por ejemplo, cada tres años, o de alguna otra manera que se ajuste al ciclo de la conferencia de examen), utilizando un mecanismo normalizado de presentación de informes, la encuesta nacional sobre la implementación de las recomendaciones de

[1] Véanse A/65/201, A/68/98, A/70/174 y A/76/135.
[2] A/75/816.

las Naciones Unidas sobre el uso responsable de las tecnologías de la información y las comunicaciones por los Estados en el contexto de la seguridad internacional (se encuentra en https://nationalcybersurvey.cyberpolicyportal.org/).

Australia reconoce la importancia de la comunidad de múltiples interesados, incluidos la sociedad civil, el sector privado, el mundo académico y la comunidad técnica, a la hora de contribuir a un ciberespacio libre, abierto, seguro, estable, accesible y pacífico. Australia propone que el programa de acción permita consultar de manera periódica e institucionalizada a las partes interesadas pertinentes.

En resumen, Australia insiste en que el programa de acción debería tener un mandato claro que se base en el marco acordado y lo reafirme; ser flexible, tanto desde el punto de vista sustantivo, ya que el marco puede seguir desarrollándose por consenso, como desde el punto de vista procedimental; apoyar los esfuerzos de implementación a través de la presentación de informes voluntarios y en la aplicación del marco a través de la creación de capacidad; y ser inclusivo, en el sentido de que las decisiones sobre asuntos relacionados con la seguridad internacional siguen siendo prerrogativa de los Estados, mientras que los debates y los grupos de trabajo están abiertos a la comunidad de múltiples partes interesadas.

Australia espera con interés seguir trabajando con el Secretario General, la Oficina de Asuntos de Desarme y los Estados Miembros para desarrollar un programa de acción eficaz, flexible e inclusivo.

## Azerbaiyán

[Original: inglés
1 de mayo de 2024]

En los últimos años, el ciberespacio ha evolucionado notablemente, lo que ofrece perspectivas para mejorar nuestra vida cotidiana, desde la seguridad hasta la velocidad de la comunicación y el uso de las tecnologías digitales. Los avances en tecnología cibernética y crítica sustentan la prosperidad futura del mundo, al tiempo que también pueden socavar la estabilidad y la previsibilidad. Por tanto, es esencial fomentar medidas de creación de capacidad, capacidades de protección suficientes y servicios digitales que contribuyan a un ciberespacio más seguro.

### Medidas adoptadas a nivel nacional para fortalecer la seguridad de la información y promover la cooperación internacional en este ámbito

Azerbaiyán apoya la labor 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), establecido en virtud de la resolución 75/240 de la Asamblea General. Como uno de los copatrocinadores de la resolución 78/237 de la Asamblea General, Azerbaiyán ha tomado varias medidas para reforzar la seguridad de la información y promover la cooperación internacional en materia de ciberseguridad.

Cabe señalar que la Estrategia de la República de Azerbaiyán sobre Seguridad de la Información y Ciberseguridad para 2023-2027, aprobada por un decreto del Presidente de la República de Azerbaiyán de fecha 28 de agosto de 2023, sirve para mejorar el nivel nacional de seguridad de la información con miras a la utilización segura de las tecnologías de la información y las comunicaciones (TIC) modernas por el Estado, la sociedad y los particulares, lo que supone el establecimiento y la aplicación de medidas para garantizar la seguridad del Estado, las redes privadas y la infraestructura crítica de información, así como la protección de los datos personales, y contribuir así a crear condiciones más favorables para la defensa de los derechos humanos y las libertades fundamentales consagrados en la Constitución de la

República de Azerbaiyán. Siendo la primera estrategia en el campo de la seguridad de la información y la ciberseguridad en la República de Azerbaiyán, se erige como un componente integral de la política del Estado en relación con las TIC y describe sus principales objetivos, direcciones, tareas prioritarias y soluciones respectivas y un plan de medidas amplias que rigen este ámbito.

Además, en el Plan de Acción de la Estrategia, en la sección 8.9.2.3., se señala "una medida continua para organizar el desarrollo de la cooperación internacional y el estudio de la experiencia internacional en el ámbito de la ciberseguridad a nivel de las entidades de la seguridad de la información, incluido el Equipo Nacional de Respuesta a Emergencias Informáticas y otros equipos de respuesta a emergencias informáticas", siendo el objetivo principal la mejora de la cooperación con los centros internacionales de equipos de respuesta a emergencias informáticas y la pertenencia a los centros internacionales de equipos de respuesta a emergencias informáticas. Actualmente se están llevando a cabo trabajos prácticos con vistas a ampliar las actividades mutuas y el intercambio de experiencias.

Cabe señalar que las Normas para Garantizar la Seguridad de la Infraestructura Crítica de Información en la República de Azerbaiyán y las Normas sobre la Estructura, Creación y Gestión del Registro de Objetos de Infraestructura Crítica de Información fueron aprobadas por las decisiones pertinentes del Gabinete de Ministros de la República de Azerbaiyán en 2023.

Además, como consecuencia de las medidas tomadas conjuntamente por el Servicio de Seguridad del Estado de la República de Azerbaiyán y la Asociación de Organizaciones de Ciberseguridad de Azerbaiyán, la posición de nuestro país en la clasificación internacional del Índice Nacional de Ciberseguridad pasó del puesto 86 al 50 en 2023.

El Servicio Estatal de Comunicación Especial y Seguridad de la Información de la República de Azerbaiyán ha elaborado un proyecto de directrices para garantizar la seguridad de la información, que se presentará a los organismos públicos con el objetivo de garantizar la seguridad de la información en las instituciones estatales, lo cual incluye el establecimiento de medidas preventivas y correctivas contra las posibles amenazas en el entorno de la información corporativa.

Se ha puesto en marcha un proyecto de ciberhigiene para mejorar la ciberresiliencia frente a las ciberamenazas y concienciar sobre el terreno a los empleados de las instituciones estatales, así como a los del sector privado y a los empresarios.

Los días 26 y 27 de octubre de 2023 se celebró un festival cibernético, el Critical Infrastructure Defense Challenge 2023, organizado conjuntamente por el Servicio Estatal de Comunicación Especial y Seguridad de la Información y el Servicio de Seguridad del Estado, cuyo objetivo era mejorar la experiencia, los conocimientos y las aptitudes de las empresas locales y extranjeras y las instituciones de los sectores público y privado que operan en el ámbito de la ciberseguridad, la infraestructura crítica y los sectores financiero y de las telecomunicaciones.

En la Conferencia Internacional sobre Ciberdiplomacia organizada por el Instituto Nacional de Investigación y Desarrollo en Informática en abril de 2023 en Rumanía, se decidió que Azerbaiyán acogería la siguiente conferencia en 2024.

Como resultado de las actividades prácticas llevadas a cabo con vistas a conformar y desarrollar el ecosistema nacional en el ámbito de la ciberseguridad, la posición de Azerbaiyán en las clasificaciones internacionales ha mejorado considerablemente. Según el índice mundial de ciberseguridad de 2020, establecido

por la Unión Internacional de Telecomunicaciones, Azerbaiyán mejoró su posición en 15 puntos, y se situó en el puesto 40 entre 194 países, con una puntuación de 89,31.

En cuanto a la colaboración internacional en el ámbito mencionado, participantes de los distintos organismos de la República de Azerbaiyán han asistido a los eventos internacionales dedicados a la cooperación en la lucha contra las ciberamenazas, el intercambio de información y las experiencias sobre incidentes de ciberseguridad, la elaboración de políticas y las estrategias en el ámbito de la ciberseguridad. Ello abarca las reuniones del Comité Especial encargado de Elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos, de carácter intergubernamental y de composición abierta, los actos celebrados en el marco de CyberEast, la Agencia de la Unión Europea para la Formación Policial y los proyectos de capacitación y alianza operacional contra la delincuencia organizada financiados conjuntamente por la Unión Europea y el Consejo de Europa.

## Canadá

[Original: inglés
16 de abril de 2024]

La tendencia a alza de la actividad malintencionada en el ciberespacio en los últimos años refuerza el impulso de trabajar eficazmente para mitigar amenazas que podrían socavar la seguridad y la estabilidad internacionales.

La necesidad de fomentar la colaboración y las iniciativas orientadas a la acción debe ir acompañada de un mecanismo equiparable de las Naciones Unidas sobre ciberseguridad. El Canadá subraya la necesidad de basarse en el acervo colectivo (las normas existentes y nuestra idea común sobre cómo se aplica el derecho internacional) y de crear un espacio en el que puedan celebrarse debates más profundos, concretos y técnicos, de manera intrínsecamente relacionada con nuestros debates en contextos plenarios. El Canadá considera que el futuro diálogo institucional periódico debe funcionar como un ciclo virtuoso de evaluaciones de amenazas, debates sobre la aplicación del marco, desarrollo de la capacidad y examen de las deficiencias que se hayan detectado y deban subsanarse. Si se trabaja en problemas de la vida real, o en hipótesis que emulen tales problemas, hay más probabilidades de arrojar luz sobre soluciones tangibles de mitigación. El futuro diálogo institucional periódico debe estar orientado a la acción y a los resultados y demostrar un progreso continuo y mensurable.

Como propietarios y operadores de la infraestructura del ciberespacio, y como nuestros ojos y oídos sobre el terreno, la comunidad multipartita está especialmente bien situada para aportar a nuestro trabajo una contribución única y de alta calidad, de manera consultiva. Garantizar una participación significativa de las partes interesadas en el futuro diálogo institucional periódico será fundamental para alcanzar nuestro objetivo común de mantener la ciberestabilidad. Involucrar a la comunidad multipartita de esta manera es también el planteamiento más prometedor para mejorar y facilitar las oportunidades de inclusión de los Estados pequeños y en desarrollo en nuestra labor. Ello, a su vez, maximiza las posibilidades de incrementar la ciberresiliencia mundial para todos. Al ser realmente **inclusivo**, el futuro diálogo institucional periódico tiene más posibilidades de contar con la aceptación que puede permitir aplicar y desarrollar de buena fe un comportamiento responsable de los Estados en el ciberespacio.

Las preocupaciones e intereses de todos los Estados, por ejemplo en relación con el desarrollo posterior del marco, deben tenerse en cuenta en el futuro diálogo

institucional periódico, mediante la participación igualitaria de los Estados en las Naciones Unidas. Las decisiones sobre cuestiones sustantivas deben adoptarse por consenso.

El Canadá reitera y se remite a las opiniones que ha expresado sobre el futuro diálogo institucional periódico en el contexto del informe del Secretario General sobre un programa de acción, tras la resolución 77/37 de la Asamblea General, de abril de 2023. Estas opiniones reflejan, principalmente, que el Canadá reconoce y agradece los informes y recomendaciones adoptados por consenso hasta la fecha (por ejemplo, los informes 2021 del Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional y el grupo de trabajo de composición abierta sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional). El Canadá considera que la mejor línea de actuación de este grupo de trabajo de composición abierta para cumplir su mandato, según lo previsto en la resolución 75/240 de la Asamblea General, consiste en tomar una decisión sobre un diálogo institucional periódico de una sola vía, permanente, orientado a la acción e inclusivo.

El Canadá agradece la oportunidad de aportar sus puntos de vista, una vez más, sobre el futuro diálogo institucional periódico. El Canadá considera que el actual mecanismo del grupo de trabajo de composición abierta no es óptimo ni suficiente para alcanzar nuestros objetivos colectivos. El Canadá no apoyaría una repetición ni renovación permanente del actual mecanismo del grupo de trabajo de composición abierta. Por el contrario, el Canadá cree firmemente que un programa de acción, elaborado en el seno del grupo de trabajo de composición abierta e, idealmente, acordado por consenso, es la mejor vía para garantizar un diálogo institucional periódico sobre ciberseguridad de una sola vía, permanente, orientado a la acción e inclusivo. Este proceso permitiría un compromiso más centrado en la aplicación de las normas y un debate más profundo sobre cómo se aplica el derecho internacional. También garantizaría una mejor coordinación orientada a la acción (no existe tal coordinación en el actual grupo de trabajo de composición abierta) entre el debate sobre la aplicación concreta del acervo y el desarrollo de capacidades específicas.

El Canadá recuerda que desde 2021 se han celebrado debates sustantivos sobre el programa de acción como futuro diálogo institucional periódico, en particular en el contexto del documento de trabajo distribuido en el seno de este grupo de trabajo de composición abierta[1]. El Canadá reconoce y apoya los llamamientos de otros Estados Miembros a tener un proceso de vía única para debatir la ciberseguridad en las Naciones Unidas. En consecuencia, el Canadá advierte contra la creación de un proceso paralelo diferente para el diálogo institucional periódico que competiría con el programa de acción que recibió el apoyo de 161 Estados Miembros a través de la resolución 78/16 de la Asamblea General. Ello supondría una duplicación indebida e innecesaria e impondría costos laborales y financieros innecesarios a los Estados Miembros.

La estructura y el funcionamiento del programa de acción se decidirán en una conferencia internacional, en la que se adoptará una declaración política. Se prevé que la Oficina de Asuntos de Desarme preste servicios de secretaría al programa de acción. Se organizarán conferencias de examen para proporcionar orientación estratégica, debates plenarios de composición abierta similares a los que existen en el marco del actual mecanismo del grupo de trabajo de composición abierta y reuniones técnicas o grupos de trabajo para coordinar los elementos de los debates temáticos que sirvan para hacer frente a amenazas específicas (por ejemplo, determinar las

[1] Véase https://documents.unoda.org/wp-content/uploads/2021/11/Working-paper-on-the-proposal-for-a-Cyber-PoA.pdf.

actividades de creación de capacidad más pertinentes para implementar normas y aplicar el derecho internacional a los programas secuestradores).

El programa de acción aprovechará las inversiones en creación de capacidad y asistencia técnica como ingredientes esenciales para fomentar el comportamiento responsable de los Estados en el ciberespacio y facilitar la cooperación entre ellos. Establecerá un compromiso regional mediante la cooperación con organizaciones regionales para aprovechar las sinergias y coordinar las iniciativas.

El programa de acción no se limitará a publicar informes de la Presidencia, sino que dará muestras de un progreso continuo y mensurable. Tratará de salvar la brecha de rendición de cuentas entre el acervo y la práctica real en materia de rendición de cuentas consolidando los compromisos y participando en mecanismos de información o examen que permitan llevar a cabo actividades óptimas de creación de capacidad a fin de potenciar el comportamiento responsable de los Estados en todo el mundo.

## Cuba

[Original: español
29 de abril de 2024]

El desarrollo de la tecnología de la información y las comunicaciones tiene un impacto cada vez mayor en todas las esferas de la sociedad. Debemos impedir que este progreso afecte la seguridad de los Estados.

Cuba reafirma que la tecnología de la información y las comunicaciones debe ser utilizadas de manera pacífica y los Estados deben comportarse de forma responsable, por el bien común de la humanidad, para promover el desarrollo sostenible de todos los países.

Ratificamos que el único camino para evitar que el ciberespacio se convierta en un teatro de operaciones militares es la cooperación mancomunada entre todos los Estados.

Resulta imperioso adoptar, en el marco de la Asamblea General de las Naciones Unidas, un instrumento internacional legalmente vinculante que complemente el derecho internacional aplicable, que proporcione respuestas a los vacíos legales en materia de ciberseguridad y que permita atender de manera efectiva los crecientes retos y amenazas que enfrentamos.

El marco adecuado para lograrlo es 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).

Debe respetarse y preservarse el papel de este grupo inclusivo y transparente para entablar el diálogo intergubernamental periódico en el ámbito de la seguridad y el uso de la tecnología de la información y las comunicaciones. Abogamos por la continuidad de las labores en ese formato, con el fin de que estas puedan aportar resultados consensuados por todos los Estados.

Todos los Estados deben respetar las normas internacionales existentes en esta esfera. El acceso a los sistemas de información o de telecomunicaciones de otro Estado deben corresponderse con los acuerdos de cooperación internacional alcanzados, sobre la base del principio del consentimiento del Estado concernido. Las formas y alcance de los intercambios deben respetar la legislación del Estado a cuyo sistema se accederá.

El uso hostil de las telecomunicaciones, con el propósito declarado o encubierto de subvertir el ordenamiento jurídico y político de los Estados, es una violación de

las normas internacionalmente acordadas en esta materia y constituye un uso ilegal e irresponsable de estos medios.

Mediante transmisiones radiales y televisivas ilegales, se ha estado agrediendo de modo permanente desde el exterior el espacio radioeléctrico cubano, difundiendo programaciones diseñadas para incitar al derrocamiento del orden constitucional establecido por el pueblo cubano.

Como promedio, durante el 2023 se transmitieron de manera ilegal contra Cuba más de 7 000 horas mensuales a través de 21 frecuencias desde el territorio de los Estados Unidos, en contravención de los propósitos y principios de la Carta de las Naciones Unidas, el derecho internacional y las disposiciones de la Unión Internacional de Telecomunicaciones.

El bloqueo económico, comercial y financiero impuesto por el gobierno de Estados Unidos contra Cuba, por más de 60 años, ha causado severas afectaciones al pueblo cubano, incluido en el uso y disfrute de las tecnologías de la información y las telecomunicaciones.

Reiteramos nuestro profundo rechazo a la imposición de medidas coercitivas unilaterales que son contrarias al derecho internacional y dificultan la asistencia, la cooperación y la transferencia de tecnologías.

En nuestra región, se reconoce el potencial de la tecnología de la información y las comunicaciones para proporcionar nuevas soluciones a los desafíos del desarrollo y fomentar un crecimiento económico sostenido, inclusivo y equitativo, así como para alcanzar la Agenda 2030 para el Desarrollo Sostenible.

Además, se destaca la necesidad de promover un entorno de tecnología de la información y las comunicaciones abierto, seguro, estable, accesible y pacífico, como se encuentra recogido en la declaración de la VIII Cumbre de la Comunidad de Estados Latinoamericanos y Caribeños, celebrada en Kingstown, en 2024.

Cuba reitera que la cooperación internacional es fundamental para enfrentar los peligros del uso indebido de las tecnologías de la información y las comunicaciones.

## Chequia

[Original: inglés
30 de abril de 2024]

Chequia está totalmente decidida a fomentar el debate mundial sobre ciberseguridad en las Naciones Unidas y agradece los avances logrados hasta la fecha tanto por los grupos de trabajo de composición abierta como por los grupos de expertos gubernamentales.

Uno de los principales logros del grupo de trabajo de composición abierta y del Grupo de Expertos Gubernamentales es que han elaborado y consolidado un marco de comportamiento responsable de los Estados en el ciberespacio.

En este contexto, Chequia considera que la aplicación del marco de comportamiento responsable de los Estados en el ciberespacio debe ser el tema central del futuro diálogo institucional. Además, Chequia apoya la creación de un mecanismo permanente, de una sola vía, inclusivo y orientado a la acción bajo los auspicios de las Naciones Unidas una vez que concluya la labor del actual grupo de trabajo de composición abierta en 2025.

Al mismo tiempo, creemos que, para entablar un futuro diálogo institucional que funcione eficazmente en beneficio de todos nosotros, es importante seguir

debatiendo sobre su forma concreta dentro del actual grupo de trabajo de composición abierta. Como comunidad internacional, tenemos en estos momentos poco más de un año para llevar a cabo este debate.

En relación con el debate en el seno del grupo de trabajo de composición abierta, Chequia desea llamar su atención sobre el hecho de que la propuesta más elaborada, debatida y también consensuada para un futuro diálogo institucional es el programa de acción para promover el comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones (TIC).

Por otro lado, creemos que la resolución 78/237, relativa a los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional, no se basa en el enfoque gradual y el consenso alcanzado en el grupo de trabajo de composición abierta en los últimos años. Parece dar prioridad a los intereses de un reducido grupo de Estados.

El debate sobre el programa de acción no ha cesado desde 2020, y Chequia ha participado activamente en él. Reconocemos el valor del debate en curso sobre el programa de acción dentro del grupo de trabajo de composición abierta para dar forma a la dirección del programa de acción y aclarar una serie de puntos que pueden resultar controvertidos. Creemos que es importante seguir debatiendo para definir el contenido y las modalidades del futuro mecanismo. A la luz de lo anterior, proponemos que se organicen reuniones entre períodos de sesiones y reuniones específicas del grupo de trabajo de composición abierta en 2024 y 2025 para centrarse en aspectos concretos del programa de acción, incluidas las consecuencias presupuestarias.

Además, Chequia desea llamar la atención sobre determinados aspectos del programa de acción que se mencionaron en el debate sobre el programa de acción y que Chequia considera las ventajas más importantes del programa de acción:

- El programa de acción aportaría estabilidad institucional al debate internacional sobre las TIC. Representaría un marco institucional permanente que sustentaría todos los debates relacionados con la cibernética en el marco de las Naciones Unidas. Ello evitaría la necesidad de debatir periódicamente la creación de un nuevo grupo de trabajo dedicado al uso de las TIC.

- El programa de acción contribuiría a la aplicación del marco de comportamiento responsable de los Estados y permitiría seguir debatiendo sobre el desarrollo del marco, si fuera necesario.

- El programa de acción serviría para poner en funcionamiento los principios de la creación de capacidad como parte de sus objetivos orientados a la acción y fomentaría la aplicación dentro de los proyectos de desarrollo de capacidades cibernéticas. Podría aprovechar las iniciativas de creación de capacidad existentes y potenciales, aumentar su visibilidad y mejorar su coordinación. Por ejemplo, podría ser beneficioso estudiar la coordinación con las actividades de creación de cibercapacidad emprendidas en otros foros, como la Unión Internacional de Telecomunicaciones.

- El programa de acción facilitaría una participación y colaboración significativas con las partes interesadas no gubernamentales. La participación del sector privado, el mundo académico y la sociedad civil aportaría una valiosa experiencia en cuestiones como la evaluación de las amenazas, la aplicación de normas, incluida la medición de los avances realizados.

- El programa de acción se ha concebido como un marco amplio, que podría englobar otras iniciativas que se hayan debatido o acordado en el seno del grupo de trabajo de composición abierta.

En cuanto a las modalidades concretas, Chequia es favorable a la idea de celebrar sesiones plenarias anuales y reuniones de grupos de trabajo técnicos especializados en el período entre sesiones.

- La creación y disolución de un grupo de trabajo concreto sería competencia exclusiva de los Estados.
- El ámbito y los trabajos preparatorios de estos debates técnicos se limitarían a los temas determinados en las sesiones plenarias. A los debates asistiría, por ejemplo, un número limitado de expertos de los gobiernos y, en su caso, otras partes interesadas como el mundo académico. En particular, estos grupos de trabajo podrían centrarse en temas como la protección de infraestructuras críticas, la respuesta a los ciberincidentes y la aplicabilidad de disposiciones concretas sobre cuestiones específicas del derecho internacional en el ciberespacio.
- Si todo ello queda bien establecido, creemos que tener grupos de trabajo técnicos entre períodos de sesiones puede hacer que nuestra labor sea mucho más eficiente y también reducir la carga de las delegaciones concretas.
- Podría ser beneficioso considerar la posibilidad de no celebrar todas las reuniones de los grupos de trabajo entre períodos de sesiones en Nueva York, sino debatir también otros lugares.

## China

[Original: chino
29 de abril de 2024]

### Opiniones del Gobierno de China sobre un futuro mecanismo permanente de diálogo institucional

Con referencia a la resolución 78/237 de la Asamblea General sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional, la postura y las opiniones del Gobierno de China sobre un futuro mecanismo permanente de diálogo institucional son las siguientes:

La cuestión de un futuro mecanismo permanente es de gran importancia para el modo de proceder de las Naciones Unidas en cuanto al desarrollo de los asuntos relacionados con la seguridad de la información. China apoya la creación de un único mecanismo futuro permanente para el diálogo institucional sobre ciberseguridad, con participación universal, en el marco de las Naciones Unidas. Llegar a un consenso sobre un futuro mecanismo permanente en el marco del grupo de trabajo de composición abierta es la única opción para todas las partes. China no apoya ningún intento de establecer un mecanismo permanente al margen del grupo de trabajo. Estamos en contra de volver a empezar de cero, ya que ello generaría divisiones en los procesos de seguridad de la información de las Naciones Unidas y alimentaría la discordia geopolítica y el enfrentamiento entre bloques. Es algo que no beneficiaría a ningún Estado Miembro.

En cuanto a la estructura y las funciones del futuro mecanismo permanente, debe consolidar los importantes logros alcanzados en el mantenimiento de los procesos de seguridad de la información de las Naciones Unidas en los últimos 26 años y buscar un desarrollo a largo plazo en el futuro. La estructura puede incluir dos partes, una de ellas “retrospectiva”, centrada en el cumplimiento y la aplicación del actual marco de comportamiento responsable de los Estados en el ciberespacio, sobre todo para enriquecer y mejorar los planes de acción para de creación de capacidad. La segunda parte debe estar orientada al futuro y centrarse en seguir el ritmo de los tiempos para

formular nuevas normas, en particular en materia de seguridad de los datos, promover la elaboración de un instrumento jurídico pertinente y proponer nuevos planes de acción para la creación de capacidades. China presentó la Iniciativa Mundial de Seguridad de los Datos para proponer soluciones prácticas a los problemas de seguridad de los datos. La Iniciativa estipula que los países no deben exigir a sus empresas que almacenen en su territorio datos generados o adquiridos en el extranjero; deben respetar la soberanía, la jurisdicción y el derecho de otros países a gestionar la seguridad de los datos y no deben acceder directamente a los datos de empresas o particulares de otros países sin la autorización legal de dichos países para hacerlo. La Iniciativa presentó propuestas específicas para la protección de infraestructura crítica y la seguridad de la cadena de suministro. Se ha distribuido como documento oficial de la Asamblea General de las Naciones Unidas. China está dispuesta a trabajar con todas las partes para promover la formulación de normas internacionales de gobernanza digital que reflejen los deseos y respeten los intereses de todas las partes.

El futuro mecanismo permanente debería estar dirigido por los Estados Miembros y, al mismo tiempo, garantizar la participación de múltiples partes interesadas, como ocurre actualmente en el grupo de trabajo de composición abierta. Las conferencias de examen podrían celebrarse cada cinco años, y podrían organizarse dos o tres sesiones plenarias cada año. Durante los tres primeros años del ciclo de examen, podrían celebrarse debates sustantivos centrados en temas concretos y adoptarse informes anuales, así como decisiones consensuadas sobre cuestiones importantes de amplio interés para los Estados Miembros. En el cuarto año del ciclo de examen, podría iniciarse el proceso preparatorio de la conferencia de examen y podrían redactarse textos de propuestas en nombre de la Presidencia. En el quinto año del ciclo de examen, podrían celebrarse debates sustantivos, principalmente sobre la base del texto de propuestas de la Presidencia, con un consenso sustantivo concluido o negociado, y podría preverse el trabajo de los siguientes cinco años.

China está dispuesta a seguir participando activamente en el proceso correspondiente y a contribuir a la creación del futuro mecanismo permanente.

China espera que estas opiniones puedan reflejarse en los informes pertinentes del Secretario General de las Naciones Unidas.

## Dinamarca

[Original: inglés
1 de mayo de 2024]

Dinamarca considera que la aplicación del marco de las Naciones Unidas de comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones (TIC) es fundamental para garantizar un ciberespacio global, abierto, estable y seguro. La comunidad internacional reconoce que el derecho internacional vigente y la Carta de las Naciones Unidas en su totalidad son aplicables en el entorno de las TIC, y Dinamarca sigue decidida a aplicar este marco en lo que respecta al ciberespacio.

Durante los últimos 20 años, se han logrado avances considerables en la elaboración de un marco consolidado de comportamiento responsable de los Estados en el ciberespacio, que incluye la aplicación del derecho internacional, normas voluntarias, creación de capacidad y medidas de fomento de la confianza. La Asamblea General ha refrendado el marco por consenso en repetidas ocasiones, la última de ellas en el informe anual sobre los progresos realizados de 2023 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).

Dinamarca, junto con la Unión Europea, considera que algunas partes de la resolución 78/237 sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional, aprobada por la Asamblea General el 22 de diciembre de 2023, se basan en un texto no consensuado. Más concretamente, el decimosexto párrafo del preámbulo y el párrafo 5 se basan en propuestas que solo cuentan con el apoyo de un grupo limitado de Estados. A Dinamarca le preocupa que este hecho pueda llevar a una reinterpretación de los documentos consensuados existentes. Por tanto, Dinamarca no ha podido apoyar la resolución 78/237.

**Sobre la solicitud relacionada con el párrafo 8 de la resolución**

Las Naciones Unidas han exigido en reiteradas ocasiones que el mecanismo sobre cuestiones cibernéticas en el contexto de la seguridad internacional sea permanente. Con la decisión adoptada por la Asamblea General en octubre de 2023 de establecer un programa de acción para promover el comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional, hemos cumplido el llamamiento mencionado.

Se han logrado avances considerables en los debates sobre el futuro mecanismo, y Dinamarca desea expresar las siguientes opiniones adicionales relativas al futuro diálogo institucional periódico.

Este diálogo institucional debería centrarse en el apoyo a la aplicación del marco normativo, como también dejó claro el grupo de trabajo de composición abierta sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional (2019-2021), que concluyó que el futuro diálogo institucional debería ser “un proceso orientado a la acción que persiguiera objetivos específicos y se basara en los resultados anteriores, y que fuera inclusivo, transparente, centrado en el consenso y basado en los resultados”[1].

El programa de acción debe proporcionar un mecanismo permanente e institucional para hacer un seguimiento de la aplicación de las normas acordadas, respaldar y promover la creación de capacidad y ofrecer recomendaciones y actualizarlas periódicamente. Al mismo tiempo, el programa de acción debe ser flexible y permitir un mayor desarrollo del marco, sobre la base de las lecciones aprendidas durante la aplicación de los compromisos existentes.

Dinamarca considera crucial reconocer que todas las partes interesadas tienen un papel importante en la configuración del futuro de la ciberseguridad. Para garantizar un diálogo inclusivo, es esencial permitir que las partes interesadas pertinentes, como las empresas, las organizaciones no gubernamentales y el mundo académico, participen oficialmente en las consultas y expongan continuamente sus puntos de vista. Ello demuestra la determinación de aprovechar la sabiduría colectiva que aportan las diversas perspectivas. Esta inclusión es vital para crear un diálogo eficaz y exhaustivo que afronte los problemas polifacéticos de la ciberseguridad.

El programa de acción permitiría celebrar reuniones oficiales anuales y organizar a lo largo del año reuniones técnicas y grupos de trabajo centrados en aspectos importantes. El futuro mecanismo debe convocar conferencias periódicas de examen para examinar el marco de comportamiento responsable de los Estados,

[1] A/75/816, párr. 74.

actualizarlo en caso necesario y proporcionar orientación estratégica para el trabajo del mecanismo.

Durante lo que queda del ciclo del grupo de trabajo de composición abierta, debería dedicarse tiempo y esfuerzo a profundizar en aspectos del programa de acción. Para garantizar una transición fluida hacia el programa de acción, resulta procedente debatir las consecuencias presupuestarias de un mecanismo permanente y determinar los agentes pertinentes en las Naciones Unidas para llevar a cabo estas funciones en el futuro.

## Egipto

[Original: inglés
26 de febrero de 2024]

### I. Introducción

1. Los Estados Miembros comparten la creciente preocupación internacional por la proliferación de usos malintencionados de las tecnologías de la información y las comunicaciones (TIC) y el desarrollo excesivo por parte de varios Estados de capacidades en materia de TIC con propósitos incompatibles con el derecho internacional y con los objetivos de mantener la estabilidad y la seguridad internacionales y que pueden afectar negativamente a la integridad de las infraestructuras de otros Estados, en detrimento de su seguridad en las esferas civil y militar.

2. Las Naciones Unidas ya han avanzado en el tratamiento de estas preocupaciones mediante las evaluaciones y recomendaciones de los Grupos de Expertos Gubernamentales de 2010, 2013, 2015 y 2021, así como las del Grupo de Trabajo de Composición Abierta de 2021 sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional[1], estableciendo así un marco acumulativo y evolutivo de comportamiento responsable de los Estados en el uso de las TIC, elaborado por estos procesos.

3. Se ha pedido a los Estados Miembros que, al utilizar las TIC, se guíen por los informes de 2010, 2013, 2015 y 2021 de los Grupos de Expertos Gubernamentales y el informe de 2021 del grupo de trabajo de composición abierta, así como por los informes anuales primero y segundo sobre los progresos realizados por el actual grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025). Además, este marco acordado ha destacado que el derecho internacional y, en particular, la Carta de las Naciones Unidas, son aplicables y fundamentales para mantener la paz y la estabilidad y fomentar un entorno de las TIC abierto, seguro, estable, accesible y pacífico.

4. El marco existente de normas, reglas y principios de comportamiento responsable de los Estados en el uso de las TIC puede reducir los riesgos para la paz, la seguridad y la estabilidad internacionales sin limitar ni prohibir acciones que, por lo demás, respeten el derecho internacional.

5. En 2020, Egipto y Francia presentaron un proyecto de programa de acción de las Naciones Unidas para fomentar el comportamiento responsable de los Estados en el uso de las TIC en el contexto de la seguridad internacional, y la propuesta ha sido desarrollada desde entonces por un grupo interregional de Estados, como se refleja en los informes finales de los Grupos de Expertos Gubernamentales y en el informe de 2021 del grupo de trabajo de composición abierta, así como en los informes anuales

[1] Véanse A/65/201, A/68/98, A/70/174, A/75/816 y A/76/135.

primero y segundo sobre los progresos realizados por el actual grupo de trabajo de composición abierta.

6. El Secretario General publicó un informe (A/78/76) en el que se consolidaban las opiniones de los Estados sobre el alcance, la estructura, los principios, el contenido, los preparativos y las modalidades para el establecimiento del programa de acción.

7. Cualquier futuro mecanismo de diálogo institucional periódico debe basarse en el acervo y en el marco acordado actual, que ha sido refrendado por consenso por la Asamblea General.

8. El nuevo mecanismo o plataforma se establecerá tras la conclusión del mandato del actual grupo de trabajo de composición abierta después de 2025. De este modo, no habrá lugar a que se produzca una duplicación de esfuerzos ni una creación de vías paralelas. Debería representar una ventanilla única y plataforma amplia bajo los auspicios de las Naciones Unidas, que abordaría cuestiones relacionadas con los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional y promovería el comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones.

9. Los Estados Miembros acordaron en principio que el mecanismo de diálogo institucional periódico tendría una única vía, estaría dirigido por los Estados y sería permanente, inclusivo, transparente y flexible[2].

## II. Objetivos y ámbito del futuro mecanismo de las Naciones Unidas para el diálogo institucional periódico

10. Servir de plataforma de diálogo institucional periódico que permitiría la participación de todos los Estados Miembros en un proceso de una sola vía, permanente, inclusivo, transparente, orientado a la acción, basado en los resultados y que actúe por consenso, que se apoye en el marco existente.

11. Fomentar un entorno de TIC abierto, seguro, estable, accesible, pacífico e interoperable,

12. Prevenir los conflictos derivados del uso de las TIC y tratar de resolver las controversias pertinentes por medios pacíficos.

13. Afianzar las herramientas cibernéticas establecidas (directorio de puntos de contacto y todas las demás propuestas que adopte el grupo de trabajo de composición abierta) con miras a mantener su funcionamiento eficaz y examinarlas, según proceda.

14. Elaborar orientaciones concretas para ayudar a los Estados Miembros a aplicar las normas, reglas y principios acordados, en particular fomentando la cooperación y la asistencia internacionales.

15. Su alcance debe centrarse en los tres pilares siguientes:

a) **Aplicación de los resultados acordados existentes**. Evaluar periódicamente la aplicación del marco acordado por los Estados Miembros mediante el examen de sus informes nacionales voluntarios sobre la aplicación, que deben seguir un modelo de informe normalizado acordado;

b) **Desarrollo del marco existente**. Detectar las lagunas y los diversos retos a los que se enfrentan los Estados Miembros en la aplicación del marco y promover recomendaciones prácticas pertinentes para responder a estos retos, así como reanudar las deliberaciones sobre cuestiones conceptuales como la aplicabilidad del

[2] A/78/265, párr. 55.

derecho intencional o la necesidad de elaborar nuevas normas y obligaciones jurídicamente vinculantes en este ámbito;

c) **Promover la creación de capacidad**. Adoptar medidas prácticas para promover la cooperación internacional y evaluar periódicamente si son necesarias acciones adicionales para responder a los retos actuales y emergentes, teniendo en cuenta la rápida evolución del entorno; intercambiar información sobre las mejores prácticas que pueden aplicarse en los planos nacional, regional e internacional (incluidos los marcos legislativos y administrativos y las medidas adoptadas para proteger la infraestructura crítica); y proporcionar apoyo concreto para la creación de capacidad basado en la propia evaluación de las necesidades de los Estados beneficiarios y de conformidad con los principios de creación de capacidad contenidos en el documento A/76/135. Podría preverse un mecanismo de financiación específico para las actividades pertinentes, incluida la posibilidad de recurrir a instrumentos existentes o nuevos, como el fondo fiduciario de donantes múltiples para la ciberseguridad del Banco Mundial.

## III. Establecimiento del futuro mecanismo de diálogo institucional periódico

16. Las opiniones y contribuciones presentadas por los Estados Miembros en el marco del actual grupo de trabajo de composición abierta sobre la propuesta de programa de acción y los informes del Secretario General de conformidad con las resoluciones 77/380 y 78/237 de la Asamblea General, así como las posibles recomendaciones pertinentes contenidas en los informes del grupo de trabajo de composición abierta, constituirán la base para el establecimiento del mecanismo en cuanto a su alcance, estructura y modalidades.

17. Los Estados Miembros deben seguir participando activamente en el actual grupo de trabajo de composición abierta establecido en virtud de la resolución 75/240 de la Asamblea General con miras a alcanzar informes de consenso, incluidas recomendaciones sobre el establecimiento del futuro mecanismo de diálogo institucional periódico.

18. El mecanismo debe seguir elaborándose y desarrollándose en el marco del actual grupo de trabajo de composición abierta, de manera que se evite cualquier duplicación de esfuerzos o la creación de procesos que compitan entre sí y se preserve el espíritu de consenso a la hora de abordar los aspectos de seguridad internacional de las TIC en las Naciones Unidas.

19. El mecanismo se establecerá tras la conclusión del mandato del actual grupo de trabajo de composición abierta en 2025 mediante las recomendaciones del informe final del actual grupo de trabajo de composición abierta, al tiempo que podría considerarse la posibilidad de establecer el futuro diálogo institucional periódico mediante una resolución consensuada de la Asamblea General basada en consultas y preparativos inclusivos y transparentes. Los Estados Miembros pueden acordar, en el seno del actual grupo de trabajo de composición abierta, establecer el mecanismo mediante una declaración política que podría ser refrendada por una resolución de la Asamblea General, incluidas las modalidades propuestas para el mecanismo. El resultado de la Cumbre del Futuro puede incluir una referencia a un acuerdo inicial sobre este asunto.

## IV. Estructura y posibles modalidades

### Reuniones periódicas

20. El mecanismo, que podría adoptar la forma de un programa de acción, debería convocar una conferencia de examen cada seis años que se centraría en los siguientes temas:

a) Examinar y revisar la aplicación del mecanismo, determinar las principales prioridades para la acción para los años siguientes y, en consecuencia, adoptar un programa de trabajo para reuniones ulteriores.

b) Estudiar si deben elaborarse por consenso normas, reglas, principios u obligaciones vinculantes adicionales para actualizar el marco.

21. El mecanismo debe convocar reuniones bienales periódicas para implementar el programa de trabajo aprobado por la conferencia de examen y hacer un seguimiento de la aplicación de las normas, reglas y principios acordados por los Estados Miembros mediante el examen de sus informes nacionales periódicos sobre la aplicación.

22. La Presidencia de cada período de sesiones convocará reuniones consultivas preparatorias antes de cada conferencia de examen y reuniones bienales de seguimiento.

23. El mecanismo acordado podrá decidir, por consenso, la celebración de reuniones entre períodos de sesiones o la creación de grupos de trabajo oficiosos que se centren en cuestiones específicas conexas, incluida la aplicabilidad del derecho internacional y la elaboración de nuevas normas, reglas y principios, y de obligaciones o instrumentos jurídicamente vinculantes, según proceda.

**Informes**

24. En el marco del mecanismo acordado, se animaría a los Estados Miembros a presentar sus informes nacionales voluntarios sobre la aplicación cada dos años de forma rotatoria, con un mínimo de un informe cada tres ciclos (cada seis años). Este proceso podría guiarse por las recomendaciones del modelo de encuesta nacional sobre la implementación de las recomendaciones de las Naciones Unidas sobre el uso responsable de las TIC por los Estados en el contexto de la seguridad internacional. Los Estados Miembros también pueden incluir en sus informes nacionales sobre la aplicación una sección en la que expongan sus prioridades y necesidades en la esfera de la creación de capacidad.

25. Cada reunión bienal y conferencia de examen aprobará por consenso un informe final, que incluirá un documento final para presentarlo al siguiente período de sesiones de la Primera Comisión para su examen y aprobación.

**Adopción de decisiones**

26. El programa de acción adoptará sus decisiones sobre cuestiones de fondo por consenso.

**Secretaría**

27. La Oficina de Asuntos de Desarme debería prestar servicios de secretaría para el mecanismo.

**Participación de las partes interesadas**

28. El mecanismo es un proceso intergubernamental en el que la negociación y la toma de decisiones son prerrogativas exclusivas de los Estados Miembros.

29. El mecanismo procurará mantener un diálogo sistemático, sostenido y sustantivo con las partes interesadas.

30. Las organizaciones no gubernamentales pertinentes reconocidas como entidades consultivas por el Consejo Económico y Social de conformidad con la resolución

1996/31, comunicarían a la secretaría su interés en participar en la labor del mecanismo.

31. Las demás organizaciones no gubernamentales interesadas pertinentes que tuvieran competencia en el ámbito y la finalidad del mecanismo también informarán a la secretaría de su interés en participar, presentando para ello información sobre el propósito, los programas y las actividades de la organización en esferas pertinentes para el ámbito del mecanismo. En consecuencia, estas organizaciones serían invitadas a participar, con arreglo al procedimiento de no objeción, en calidad de observadores en los períodos de sesiones oficiales del mecanismo.

32. Las partes interesadas acreditadas podrán asistir a las reuniones oficiales del programa de acción, formular declaraciones orales durante una sesión dedicada a las partes interesadas y presentar aportaciones por escrito. Se alentará a los Estados Miembros a utilizar el procedimiento de no objeción con criterio, teniendo en cuenta el espíritu de inclusividad.

33. Cuando un Estado Miembro tenga una objeción a una organización no gubernamental, deberá comunicarla a la Presidencia del mecanismo y deberá dar a conocer voluntariamente a la Presidencia del grupo de trabajo los motivos generales de la objeción. La Presidencia remitirá la información recibida a los Estados Miembros que la soliciten.

34. La Presidencia organizará reuniones consultivas oficiosas con las partes interesadas en el período entre sesiones.

35. El mecanismo podrá facilitar la coordinación con las iniciativas regionales y subregionales pertinentes, incluso mediante su posible participación y contribuciones.

## Estados Unidos de América

[Original: inglés
1 de mayo de 2024]

### Introducción

Los Estados Miembros de las Naciones Unidas han reconocido que las TIC pueden utilizarse con fines incompatibles con el mantenimiento de la paz y la estabilidad internacionales. A lo largo de muchos años, los Estados se han reunido bajo los auspicios de las Naciones Unidas para debatir y abordar esta cuestión. Mediante la afirmación por consenso de los informes del Grupo de Expertos Gubernamentales sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional y 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), los Estados han convergido en torno a un marco de comportamiento responsable de los Estados en el uso de las TIC. Este marco para reforzar la estabilidad internacional incluye el respeto del derecho internacional pertinente, incluida la Carta de las Naciones Unidas, y un conjunto de normas no vinculantes y medidas de fomento de la confianza.

Si bien el marco ha recibido apoyo mundial, su éxito depende de que los Estados hagan suyos sus elementos y los apliquen. Como se articuló en primer lugar en el informe de consenso del Grupo de Expertos Gubernamentales de 2015, los Estados han afirmado la necesidad de establecer un diálogo institucional periódico con amplia participación bajo los auspicios de las Naciones Unidas[1]. Basándose en ese esfuerzo,

[1] A/70/174 , párr. 18.

el grupo de trabajo de composición abierta ha reafirmado continuamente desde entonces la necesidad de que los Estados trabajen en pro del establecimiento de un mecanismo para el futuro diálogo institucional[2].

Además, como se señala en el último informe consensuado sobre los progresos realizados por el grupo de trabajo de composición abierta, los Estados acordaron un conjunto inicial de elementos comunes de diálogo institucional periódico, y también acordaron seguir debatiendo el futuro programa de acción. Los Estados acordaron, lo que es más importante, que el futuro diálogo institucional periódico debería tomar "como base de su trabajo los acuerdos consensuados sobre el marco de comportamiento responsable de los Estados"[3]. Los Estados también acordaron que el futuro diálogo debería ser unidireccional, dirigido por los Estados y permanente[4]. Los Estados llegaron además a la conclusión de que el mecanismo debía ser abierto, inclusivo, transparente, sostenible y flexible[5] para que pudiera adaptarse según fuera necesario a la rápida evolución del panorama de las ciberamenazas. En su informe publicado en abril de 2023 (A/78/76), el Secretario General subrayó la urgencia de establecer el programa y destacó muchas de las mismas cuestiones abordadas por los elementos comunes indicados en el informe anual de 2023 sobre los progresos realizados por el grupo de trabajo de composición abierta, en particular que el marco "debe servir de base de referencia" para el programa de acción[6]. En el informe, el Secretario General también llegó a la conclusión de que muchos Estados valoran la participación inclusiva y significativa de las partes interesadas no gubernamentales[7]. Los Estados siguieron pidiendo una participación significativa de las múltiples partes interesadas en las sesiones oficiales y entre períodos de sesiones del grupo de trabajo de composición abierta.

A lo largo de los dos últimos años, los Estados han convergido en torno al programa de acción como un futuro mecanismo permanente para los debates de la Primera Comisión de las Naciones Unidas sobre cuestiones cibernéticas. Más recientemente, casi todos los Estados Miembros de las Naciones Unidas votaron a favor de la resolución 78/16, en la que la Asamblea General estableció de forma decisiva el mecanismo bajo los auspicios de las Naciones Unidas tras concluir la labor del actual grupo de trabajo de composición abierta sobre la seguridad de las TIC y de su uso.

Como se indica en la resolución, el programa de acción servirá de mecanismo permanente, aunque flexible, en las Naciones Unidas para avanzar en el trabajo del marco para mejorar la paz y la seguridad en el ciberespacio, en particular colaborando de forma significativa con la comunidad de múltiples partes interesadas y facilitando la creación de capacidades a través del papel de las Naciones Unidas como plataforma de intercambio de información.

### Ámbito del programa de acción

En la resolución 77/37 de la Asamblea General se definieron el ámbito y el mandato del programa de acción del siguiente modo:

> Un mecanismo permanente, inclusivo y orientado a la acción para analizar las amenazas existentes y potenciales; apoyar las capacidades y los esfuerzos de los Estados para cumplir y promover los compromisos guiados por el marco de comportamiento responsable de los Estados, que incluye normas voluntarias y

[2] A/75/816, párrs. 70 a 74, y A/78/265, párr. 52.
[3] A/78/265, párr. 55 c).
[4] *Ibid*., párr. 55 a).
[5] *Ibid*., párr. 55 d).
[6] A/78/76, párr. 42.
[7] A/78/76, párr. 40.

no vinculantes para la aplicación del derecho internacional al uso que hacen los Estados de las tecnologías de la información y las comunicaciones, medidas de fomento de la confianza y creación de capacidad, como se afirma en la resolución 76/19 de la Asamblea General, los informes de 2010, 2013, 2015 y 2021 de los grupos de expertos gubernamentales, el informe de 2021 del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional y el primer informe anual 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) sobre los progresos realizados; analizar y, si correspondiera, desarrollar este marco; promover la interacción y la cooperación con las partes interesadas; y revisar periódicamente los progresos realizados en la implementación del programa de acción, así como su labor futura[8].

En su resolución 78/16, la Asamblea General reafirmó los objetivos del programa de acción articulados en la resolución 77/37 y también decidió que el mecanismo tendría los elementos comunes descritos en el informe de 2023 sobre los progresos realizados por el grupo de trabajo de composición abierta. Además, la Asamblea decidió que el ámbito, la estructura, el contenido y las modalidades del programa de acción se basarían en los resultados consensuados del grupo de trabajo de composición abierta.

En las distintas resoluciones sobre el programa de acción y las resoluciones consensuadas donde se reafirmaban los informes del Grupo de Expertos Gubernamentales y del grupo de trabajo de composición abierta, los Estados han afirmado repetidamente que esperaban que los países se guiaran en sus acciones por las evaluaciones y recomendaciones de los grupos de expertos gubernamentales de 2010, 2013, 2015 y 2021, así como las del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional de 2021, junto con los productos consensuados del actual grupo de trabajo de composición abierta (p. ej., los informes anuales primero y segundo sobre los progresos realizados), y en particular “el marco acumulativo y evolutivo de comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones que han ido elaborando y aprobando por consenso en esos procesos”[9]. Este marco consensuado, articulado por los informes consensuados del Grupo de Expertos Gubernamentales y el grupo de trabajo de composición abierta y refrendado en repetidas ocasiones por todos los Estados Miembros, constituye la base del programa de acción.

Los Estados Miembros establecerán la dirección del programa de acción y la actualizarán con el tiempo, manteniendo un enfoque prioritario en la aplicación práctica y la labor de creación de capacidad dedicada a la aplicación del marco. El carácter permanente del programa de acción lo convertirá en un recurso duradero para los Estados en estos esfuerzos.

Como mecanismo permanente, el programa de acción también debe tener la flexibilidad necesaria para hacer frente a futuras amenazas y la agilidad para evaluar la evolución de las necesidades de los Estados y las mejores prácticas para hacer frente a estas amenazas. Dentro del programa de acción, los Estados también podrán considerar si el marco consensuado debe evolucionar con el tiempo y de qué manera.

Las partes interesadas no estatales serán parte integrante del proceso del programa de acción. En casi todas las iniciativas de creación de capacidad, nacionales

[8] Resolución 77/37 de la Asamblea General, párr. 1.
[9] Resolución 78/16 de la Asamblea General, octavo párrafo del preámbulo.

o internacionales, intervienen actividades y conocimientos especializados del sector privado, la sociedad civil, el mundo académico y otros interesados no estatales. El programa de acción debe contar con modalidades de participación de las partes interesadas que sean lo más inclusivas posible para aprovechar al máximo la experiencia de estas partes.

**Establecimiento de un programa de acción**

Los Estados Miembros deben aspirar a una transición fluida al programa de acción en 2025 una vez que concluya la labor del grupo de trabajo de composición abierta (2021-2025). Dicha transición debe verse facilitada por un informe final del grupo de trabajo de composición abierta que reafirme el mandato del programa tal y como se define en la resolución 77/37 de la Asamblea General con el marco consensuado como base, articule su estructura orientada a la acción y sus métodos de trabajo, defina los ámbitos de trabajo prioritarios, confirme un planteamiento lo más inclusivo posible de la participación de las partes interesadas y defina los siguientes pasos y el calendario detallado para la puesta en marcha oficial del programa en 2026.

Para definir plenamente las modalidades del programa de acción, puede ser necesario organizar una reunión preparatoria o un proceso preparatorio adicional. Además, si el grupo de trabajo de composición abierta no logra alcanzar un consenso sobre un informe final, se necesitará una "conferencia internacional"[10] más amplia u otro proceso preparatorio establecido a través de la Asamblea General para cumplir la directiva indicada en la resolución 78/16 de poner en marcha el programa para 2026. Las reuniones del programa deben comenzar en 2026 para garantizar la continuidad de estos importantes debates multilaterales.

Dado el mandato propuesto del programa de acción para abordar las dimensiones de paz y seguridad del uso de las TIC, este se establecerá de forma natural en el marco de la Primera Comisión de las Naciones Unidas. La Oficina de Asuntos de Desarme es una secretaría lógica para este futuro mecanismo. El programa debe funcionar, en la medida de lo posible, con los recursos presupuestarios existentes.

**Estructura**

La estructura del programa de acción debe abarcar: grupos de trabajo técnicos que se reúnan tres o cuatro veces al año, reuniones plenarias anuales y conferencias periódicas de examen. El programa contaría con el apoyo de una oficina de secretaría dentro de la Oficina de Asuntos de Desarme.

Los grupos de trabajo técnicos del programa de acción son la esencia de su naturaleza orientada a la acción, no una característica opcional. Para que estos grupos sean lo más inclusivos posible, se invitaría a todos los Estados interesados a colaborar en grupos específicos para elaborar recomendaciones concretas que sirvan para aplicar el marco. Estas recomendaciones se incluirían en informes que se someterían a la consideración del pleno y, en última instancia, de la Asamblea General.

Estos grupos de trabajo deben tener una composición interregional y han de adoptar un planteamiento transversal para aplicar el marco, y elaborar recomendaciones, evaluaciones y mejores prácticas sobre cuestiones como:

- Defender las infraestructuras vitales
- Facilitar la cooperación entre Estados tras un ciberincidente grave

[10] Resolución 77/37 de la Asamblea General, párr. 3.

- Formas de mejorar la rendición de cuentas por el comportamiento irresponsable del Estado en el ciberespacio
- Intercambio de información sobre la evolución del panorama de las ciberamenazas
- Mejorar la capacidad de los Estados para disuadir a los infractores y evitar las amenazas para las TIC

Los debates temáticos facilitarían una discusión transversal sustantiva sobre la aplicación del marco que acabaría con los compartimentos estancos tradicionales de las amenazas, las normas, el derecho internacional y la creación de capacidades. En el grupo de trabajo de composición abierta, los Estados insistieron repetidamente en que estos temas se entrecruzan y deben considerarse de forma conjunta. Los Estados también están de acuerdo en que la creación de capacidades, en particular, es transversal a todos los temas. Dar prioridad al debate sobre las necesidades de creación de capacidad en el seno de los grupos de trabajo de aplicación dará lugar a recomendaciones realistas y viables y acelerará la aplicación.

La reunión plenaria anual debe tener el mandato de evaluar los avances de los grupos de trabajo técnicos, sacar adelante las recomendaciones de dichos grupos, estudiar las amenazas en curso y emergentes y considerar la situación de iniciativas prácticas como las medidas de fomento de la confianza. En caso necesario, el pleno podrá orientar a los grupos de trabajo técnicos y las iniciativas prácticas.

La conferencia de examen periódica debe reunirse cada tres o cuatro años (sustituyendo a la reunión plenaria anual durante los años de la conferencia) para que todos los Estados Miembros evalúen la evolución del panorama de las ciberamenazas y los resultados de los grupos de trabajo y las iniciativas del programa de acción, actualicen el marco según sea necesario y proporcionen orientación estratégica y mandatos a los futuros plenos, grupos de trabajo y otras iniciativas del programa. Este examen periódico del programa daría a los Estados la flexibilidad necesaria para adaptar el programa en función de la evolución de las circunstancias.

Cada año, tras la puesta en marcha del programa de acción en 2026, la Primera Comisión reafirmaría los resultados consensuados de las reuniones anuales del programa mediante una resolución o decisión. La Primera Comisión también confirmaría los resultados de las conferencias de examen periódicas cuando se celebren.

La secretaría del programa de acción, a cargo de la Oficina de Asuntos de Desarme, tendría el mandato de ayudar a la administración de las distintas reuniones del programa; mantener plataformas de intercambio de información, mecanismos de comunicación y archivos; y administrar iniciativas y proyectos prácticos como el directorio de puntos de contacto, el repositorio de amenazas y los portales de intercambio de información.

**Creación de capacidad**

Dado que los países se encuentran en todas las fases de desarrollo de sus competencias y conocimientos cibernéticos, las Naciones Unidas han reconocido que "la creación de capacidad es esencial para la cooperación de los Estados y el fomento de la confianza en la esfera de la seguridad de las TIC"[11]. Las Naciones Unidas desempeñan una función clave para convocar, coordinar y poner de relieve el abanico de agentes de múltiples partes interesadas que participan activamente en la creación de capacidad sobre cuestiones cibernéticas pertinentes, así como en la ejecución de

[11] *Ibid*., vigésimo párrafo del preámbulo.

programas específicos de creación de capacidad siguiendo las directrices de los Estados Miembros.

La función principal de creación de capacidad del programa de acción debe estar directamente vinculada a los esfuerzos de los Estados a nivel nacional para aplicar el marco. El programa de acción también debería facilitar debates específicos sobre los tipos de actividades de creación de capacidad que necesitan los Estados para aplicar el marco, con el fin de garantizar que sus iniciativas se ajustan fielmente al abanico de necesidades de los Estados. En otras palabras, debe tener como objetivo aumentar la conciencia internacional sobre la importancia de la creación de cibercapacidad para respaldar el marco y facilitar la coordinación y el intercambio de información sobre la disponibilidad de programas de creación de cibercapacidad junto a otros interesados, a la vez que proporciona orientación y mejores prácticas que los Estados podrían utilizar a nivel nacional o interno para aplicar el marco.

Los Estados Unidos reconocen que muchos Estados siguen sin conocer en profundidad el marco y la importancia que tiene. Muchos carecen también de la capacidad de ciberseguridad a nivel nacional necesaria para aplicar el marco, incluidas las autoridades y capacidades internas vinculadas a las normas de apoyo y las medidas de fomento de la confianza. Existen distintas entidades, pertenecientes a las Naciones Unidas o ajenas a ellas, con experiencia en ámbitos como las políticas y estrategias nacionales de ciberseguridad, la gestión de ciberincidentes y la protección de infraestructura crítica, la legislación nacional sobre ciberdelincuencia, la cultura de la ciberseguridad, las normas de ciberseguridad y la coordinación y el contacto con los donantes internacionales con fines de asistencia internacional en materia de ciberseguridad. El programa de acción no debe duplicar ni sustituir los esfuerzos existentes. Todos estos programas, que en su mayoría cuentan con muchas partes interesadas, mejoran la situación de seguridad de los Estados y, en última instancia, permiten la aplicación del marco, aunque quedan fuera del mandato del programa de acción.

**Participación de múltiples partes interesadas**

Los Estados deberían conservar la autoridad exclusiva para tomar decisiones dentro del programa de acción. No obstante, las partes interesadas no gubernamentales, entre las que se incluyen la sociedad civil, el mundo académico, los órganos regionales e internacionales y el sector privado, desempeñan una función positiva en los foros multilaterales aportando su experiencia a los debates oficiales y contribuyendo a los esfuerzos de creación de capacidad. Las partes interesadas no estatales pertinentes deben tener la oportunidad de participar activamente en el programa de acción y contribuir a él en calidad de observadores, sin derecho de voto. Los conocimientos especializados de las partes interesadas no gubernamentales serán especialmente importantes en los grupos técnicos o de trabajo. Estos grupos de trabajo técnicos facilitarán una colaboración más profunda y práctica con distintas partes interesadas no estatales. Las partes interesadas también podrían presentar informes periódicos sobre sus esfuerzos para aplicar iniciativas centradas en el marco, en particular sobre creación de capacidad.

Para que el programa de acción incluya en la mayor medida posible a las partes interesadas, en particular en sus grupos de trabajo técnicos subsidiarios, las modalidades deben basarse en las normas de referencia existentes para la participación de las partes interesadas, incluida la transparencia en cuanto a las objeciones de los Estados y un proceso para evaluar las posibles exclusiones. Por ejemplo, los Estados pueden tomar como modelo el Grupo de Trabajo de Composición Abierta sobre el Envejecimiento. Las modalidades de ese Grupo brindan a los Estados Miembros la oportunidad de oponerse a la participación de una

organización, pero exigen que las objeciones se expongan públicamente para que los Estados Miembros las conozcan y que se lleve a cabo después una votación para determinar si las organizaciones con respecto a las que se ha objetado deben ser excluidas. Las organizaciones a las que no se oponga ningún Estado Miembro en la primera ronda quedan automáticamente autorizadas a participar en la sesión oficial[12].

Además de las consideraciones sobre cómo se acredita a las partes interesadas para asistir a las reuniones del programa de acción, las modalidades también deben proporcionar orientación sobre cómo pueden contribuir en la práctica las partes interesadas acreditadas a los debates del programa. En este sentido, podría servir de modelo el Comité Especial encargado de Elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos. Sus modalidades permiten la participación de múltiples partes interesadas de distintas formas, entre ellas:

- La asistencia a cualquier sesión oficial pública.
- En función del tiempo disponible, la realización de declaraciones orales, al término de los debates de los Estados Miembros, sobre cada tema sustantivo del programa. Dado el limitado tiempo disponible en las reuniones, las múltiples partes interesadas pueden considerar la posibilidad de seleccionar entre ellas a los portavoces, de forma equilibrada y transparente, teniendo en cuenta la representación geográfica equitativa, la paridad de género y la diversidad de las múltiples partes interesadas participantes.
- La presentación de material escrito con limitaciones en el número de palabras. Estas aportaciones se publican en el idioma original en el sitio web del Comité Especial[13].

El programa de acción también debe aprovechar la experiencia y el trabajo en curso a nivel regional. Permitir que estas entidades participen en los debates sobre el programa de acción, en calidad de partes interesadas, ayudaría a que el trabajo a nivel de las Naciones Unidas se integrara mejor con los esfuerzos regionales y tuviera en cuenta los retos y contextos regionales específicos.

## Estonia

[Original: inglés
30 de abril de 2024]

De acuerdo con el mandato de la Asamblea General en su resolución 78/237, Estonia desea exponer su postura nacional sobre el futuro diálogo institucional periódico sobre la seguridad de las tecnologías de la información y las comunicaciones (TIC) y de su uso.

En los últimos años, las amenazas en el uso de las TIC en el contexto de la seguridad internacional han seguido intensificándose y evolucionando de manera importante en el complicado entorno geopolítico actual. El aumento de las amenazas en el uso de las TIC está dando lugar a retos cada vez mayores relacionados con los efectos negativos sobre el desarrollo económico y social y tienen consecuencias para la estabilidad nacional e internacional. Estas consecuencias siguen siendo prioritarias en los debates multilaterales, como ilustra el trabajo del Grupo de Expertos Gubernamentales y del grupo de trabajo de composición abierta.

[12] Como se articula en la sección F del documento A/AC.278/2011/2.
[13] Véase A/AC.291/6, párr. 3.

Tras el amplio respaldo de un grupo interregional de países al establecimiento de un programa de acción, apoyamos el programa de acción como mecanismo institucional permanente en el seno de la Primera Comisión, centrado en la aplicación del marco acordado de comportamiento responsable de los Estados en el ciberespacio, y que permite al mismo tiempo el desarrollo ulterior del marco, si procede. Creemos que este diálogo institucional periódico contribuiría a reducir las tensiones, prevenir los conflictos y fomentar el uso con fines pacíficos.

Esta postura nacional es una actualización de la contribución nacional de Estonia incluida en el informe del Secretario General sobre el programa de acción (A/78/76), que se basa, entre otras cosas, en los progresos reflejados en la resolución 78/16 de la Asamblea General y en los debates del grupo de trabajo de composición abierta (2021-2025).

1. **El programa de acción debería basarse en el acervo existente y en el marco de comportamiento responsable de los Estados, centrándose en el uso de las TIC por los Estados en el contexto de la paz y la seguridad internacionales.** Estonia considera que las TIC deben emplearse de manera coherente con los objetivos de mantenimiento de la estabilidad y la seguridad internacionales y de conformidad con el acervo acordado y el marco de comportamiento responsable de los Estados. Subrayamos que los Estados Miembros deben guiarse en el uso de las TIC por los informes de 2010, 2013, 2015 y 2021 de los Grupos de Expertos Gubernamentales y el informe de 2021 del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional. El mecanismo del programa de acción debería basarse en estas premisas y guiarse por el objetivo de preservar un entorno de las TIC abierto, estable, seguro, accesible y pacífico. Estonia considera que varias iniciativas existentes o propuestas, como el directorio mundial de puntos de contacto, ofrecerían un apoyo fundamental al funcionamiento eficaz del formato del programa de acción.

2. **El programa de acción debería tener un formato neutral que garantice la estabilidad institucional.** Desde la perspectiva de un Estado pequeño, es necesario tener claridad y estabilidad institucional respecto a los procesos posteriores relacionados con los debates sobre el uso que hacen los Estados de las TIC. Estonia aboga así por el establecimiento de una estructura permanente única para proseguir los debates del grupo de trabajo de composición abierta, una vez finalizada la labor del actual grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025). Apoyamos la continuación de los debates sobre la estructura, las modalidades y el calendario para establecer el programa de acción como mecanismo para promover el comportamiento responsable de los Estados en el uso de las TIC, teniendo en cuenta las opiniones de todos los Estados Miembros. Estonia apoya la opción de establecer el mecanismo a través de una conferencia internacional, como se acuerda en la resolución 77/37 de la Asamblea General, no más tarde de 2026. Estonia cree que el formato del programa de acción propuesto eliminaría la necesidad de que la Asamblea debatiera la creación de nuevos procesos sobre cuestiones cibernéticas cada dos, tres o cuatro años. Esperamos que los Estados Miembros consideren el marco del programa de acción como un marco útil y neutral y que no haya necesidad de establecer procesos paralelos.

3. **El programa de acción debería ofrecer un marco holístico para avanzar en los diversos temas propuestos en el grupo de trabajo de composición abierta de forma inclusiva.** Acogemos con satisfacción el creciente interés de los Estados Miembros por contribuir a los diversos temas que se abordan en los debates en curso en las reuniones del grupo de trabajo de composición abierta. Los actuales debates del grupo de trabajo de composición abierta han sido sustanciales y distintos Estados

Miembros han propuesto una serie de ideas. Creemos que el marco del programa de acción podría ofrecer a los Estados Miembros un lugar al que acudir para plantear cuestiones relacionadas con las TIC y la paz y la seguridad internacionales. Por tanto, el programa de acción podría ofrecer un marco holístico para que estas ideas se presentaran y analizaran con mayor detalle.

4. **El programa de acción también debería incluir modalidades claras y transparentes para la participación efectiva de la comunidad de las múltiples partes interesadas, con el fin de poder beneficiarse aún más de su experiencia y conocimientos.** La participación de la comunidad de múltiples partes interesadas ayudará a los Estados Miembros a aplicar el marco de comportamiento responsable de los Estados y a diseñar y poner en práctica iniciativas de creación de capacidad en función de las necesidades para aumentar la ciberresiliencia a escala mundial. Del mismo modo, el programa de acción también podría mejorar la participación regional a través de la cooperación con organizaciones regionales y temáticas para aprovechar iniciativas pertinentes ya existentes.

5. **El programa de acción debe permitir un formato más flexible, aunque específico, para seguir debatiendo sobre el marco de comportamiento responsable de los Estados.** Estonia desearía subrayar que el diseño del marco del programa de acción también debería tener en cuenta los retos relativos a las capacidades limitadas de los Estados pequeños y, por lo tanto, desarrollarse a partir de expectativas razonables en cuanto a la carga de trabajo prevista:

a) Proponemos que entre los elementos del mecanismo del programa de acción se incluyan sesiones plenarias anuales para tratar temas relacionados con los principales pilares del marco de comportamiento responsable de los Estados;

b) También apoyamos los debates específicos con un formato de grupos de trabajo abiertos a todos los participantes interesados, que incluyan, entre otros temas, las amenazas, la creación de capacidades, el fomento de la confianza, las normas y el derecho internacional. Otra opción podría ser centrar estos grupos de trabajo en asuntos más temáticos como la protección de infraestructura crítica. La participación en los grupos de trabajo debe ser voluntaria y la creación de tales líneas de trabajo sería decidida por los Estados en sesiones plenarias anuales;

c) También apoyamos la organización de **conferencias de examen** (por ejemplo, cada cuatro años), que permitirían a los participantes hacer balance de los progresos realizados y considerar otras posibles modificaciones del mandato, así como de la organización del trabajo o del programa de acción.

6. Entre otros temas, **el programa de acción debe ofrecer un marco inclusivo para los debates sobre el derecho internacional.** Estonia acoge con satisfacción los debates cada vez más activos y sustanciales sobre el derecho internacional y su aplicación al uso de las TIC por los Estados. Los Estados Miembros se beneficiarían de una comprensión más profunda y de opiniones compartidas sobre la manera en que se aplican las normas existentes, así como de un análisis más detallado de las posibles lagunas. El programa de acción sería idóneo para ofrecer un lugar inclusivo en el que proseguir estos debates. En particular, el programa de acción podría ofrecer una plataforma para los siguientes elementos de debate sobre derecho internacional: a) continuación de los debates sobre cómo se aplica el derecho internacional al ciberespacio; b) puesta en común de las opiniones nacionales; c) reuniones específicas sobre cómo se aplica el derecho internacional en el uso de las TIC, centradas en temas específicos para permitir una elaboración más detallada; d) exposiciones informativas de expertos; e) debates basados en hipótesis; y f) creación de capacidad en materia de derecho internacional.

7. **El programa de acción debería estar orientado a la acción y centrarse particularmente en la creación de capacidad.** Una parte esencial de los futuros debates debería ser la aplicación del marco acordado de comportamiento responsable de los Estados. El programa de acción también podría fomentar la presentación voluntaria de informes sobre las iniciativas nacionales de aplicación, lo que contribuiría a muchos objetivos como el fomento de la confianza, la transparencia y la cartografía de capacidades y necesidades. El programa de acción debería hacer balance de las iniciativas existentes en materia de creación de capacidad de forma bien coordinada y complementaria. Por ejemplo, el diseño del programa de acción debería tomar nota de los análisis y recursos existentes, como el portal Cybil y los análisis de CyberNet (Unión Europea) de los proyectos de creación de cibercapacidad de los Estados miembros de la Unión Europea.

## Federación de Rusia

[Original: ruso
9 de abril de 2024]

**Documento conceptual sobre un grupo de trabajo permanente de composición abierta con función decisoria sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso**

**Coautores: República de Belarús, Burkina Faso, República de Burundi, República de Cuba, Estado de Eritrea, Federación de Rusia, República de Malí, República de la Unión de Myanmar, República de Nicaragua, República Árabe Siria, República Popular Democrática de Corea, República del Sudán, Venezuela (República Bolivariana de), República de Zimbabwe**

Los debates en el seno del grupo de trabajo de composición abierta de las Naciones Unidas sobre la seguridad de las tecnologías de la información y las comunicaciones (TIC) y de su uso (2021-2025) han puesto de manifiesto la demanda de la comunidad internacional de que se establezca un único mecanismo permanente de toma de decisiones sobre esta cuestión bajo los auspicios de las Naciones Unidas. Creemos que el formato óptimo para un mecanismo de este tipo es un grupo de trabajo de composición abierta, que ha demostrado en la práctica su eficacia y pertinencia.

El mandato de un futuro grupo de trabajo permanente de composición abierta con función decisoria debe centrarse en seguir promoviendo un entorno de TIC abierto, seguro, estable, accesible y pacífico mediante la aplicación práctica de los acuerdos alcanzados en el grupo de trabajo de composición abierta 2021-2025. El mandato abarca las siguientes cuestiones:

- El desarrollo continuo de reglas, normas y principios jurídicamente vinculantes sobre el comportamiento responsable de los Estados y el establecimiento de mecanismos eficaces para su aplicación, como elementos de un futuro tratado universal para garantizar la seguridad de la información internacional;
- El desarrollo de una idea común sobre cómo se aplica el derecho internacional al uso de las TIC y cómo pueden adaptarse las normas existentes a las especificidades del espacio de la información (su dimensión transfronteriza, el anonimato y la posibilidad de introducir funciones ocultas);
- La elaboración y aplicación de medidas de fomento de la confianza y de mecanismos de cooperación práctica entre los Estados, por ejemplo, mediante canales de comunicación establecidos entre entidades u órganos autorizados y un directorio intergubernamental mundial de puntos de contacto, con el fin de contrarrestar las amenazas a la seguridad de la información relacionadas con las

TIC y su uso, y de prevenir los conflictos interestatales en el espacio mundial de la información;

- El establecimiento de mecanismos y programas para ayudar a los Estados a mejorar la capacidad de proteger sus recursos nacionales de información, teniendo en cuenta las necesidades específicas.

Los siguientes principios deben sustentar un futuro grupo de trabajo permanente de composición abierta:

- Apertura, inclusividad, democracia y transparencia;
- El liderazgo de los Estados en la promoción del diálogo sobre la seguridad en el uso de las TIC por los Estados, bajo los auspicios de la Primera Comisión de la Asamblea General de las Naciones Unidas;
- Cumplimiento de los principios de la Carta de las Naciones Unidas (igualdad soberana de los Estados, no uso de la fuerza ni de la amenaza de la fuerza y arreglo pacífico de las controversias internacionales);
- Cualquier decisión se toma por consenso y únicamente por los Estados;
- Las iniciativas internacionales para garantizar la seguridad de las TIC y de su uso no deben duplicarse en varias plataformas de negociación de las Naciones Unidas;
- Continuidad con los resultados consensuados y las recomendaciones de anteriores grupos de trabajo de composición abierta y grupos de expertos gubernamentales;
- Flexibilidad y capacidad de evolucionar a medida que cambian las necesidades de los Estados y surgen nuevos retos para la seguridad de las TIC.

Cuestiones de procedimiento:

- Todas las decisiones que se tomen en el seno del grupo de trabajo permanente de composición abierta deben ser aprobadas por consenso entre los Estados (este parámetro debe figurar claramente en la resolución de la Asamblea General por la que se crea el grupo de trabajo permanente de composición abierta);
- Calendario: el grupo de trabajo permanente de composición abierta debe empezar a trabajar cuando concluya la labor del actual grupo de trabajo de composición abierta y celebrar dos períodos de sesiones oficiales al año en la Sede de las Naciones Unidas (Nueva York) (todos los Estados Miembros deben estar representados sin excepción);
- Formato de presentación de informes: informes sobre los progresos realizados a la Asamblea General de las Naciones Unidas, adoptados por consenso una vez cada dos años;
- Estructura: en caso necesario, los Estados Miembros de las Naciones Unidas pueden decidir crear subgrupos subsidiarios para abordar aspectos específicos del mandato de forma más detallada y profunda. No obstante, las reuniones de estos subgrupos no deben celebrarse simultáneamente, para garantizar la plena participación de todas las delegaciones;
- Gobernanza: las labores del grupo de trabajo permanente de composición abierta estarán dirigidas por una mesa, compuesta por una Presidencia, dos Vicepresidencias, una Relatoría y, en caso necesario, las Presidencias de los subgrupos (también con rango de Vicepresidencias). La composición de la mesa será aprobada por consenso cada dos años por los Estados sobre la base de una

distribución geográfica equitativa, por rotación de cada uno de los grupos regionales.

Sería aconsejable dotar al grupo de trabajo permanente de composición abierta de un mecanismo para formalizar rápidamente las decisiones a medida que se vayan acordando (por el procedimiento de acuerdo tácito y posterior aprobación en el siguiente período de sesiones). Deben tomarse medidas prácticas para mantener un intercambio continuo de información entre los Estados a través de un portal electrónico adecuado.

Sería útil prever que el grupo de trabajo permanente de composición abierta coopere con las organizaciones y asociaciones regionales pertinentes mediante consultas de su Presidencia con grupos de países y mediante reuniones entre períodos de sesiones celebradas con sus representantes una vez al año.

La participación de los agentes no estatales (organizaciones no gubernamentales, comunidad empresarial y comunidades científica y académica) en la labor del grupo de trabajo permanente de composición abierta debe ser de carácter puramente consultivo e informal; por ejemplo, a través de reuniones entre períodos de sesiones una vez al año. El derecho a asistir a actos oficiales en calidad de observadores solo se concederá a los agentes no estatales acreditados (acordados por consenso entre los Estados).

## Francia

[Original: francés
30 de abril de 2024]

### I. Introducción

Hace más de 20 años que los Estados vienen reconociendo que la tecnología de la información y de las comunicaciones (TIC) es un catalizador del progreso humano y del desarrollo, pero que también puede utilizarse con fines incompatibles con el objetivo de mantener la estabilidad y la seguridad internacionales.

Desde 2003, la Primera Comisión de la Asamblea General ha creado una serie de grupos de trabajo que han abordado el mantenimiento de la paz, la seguridad y la estabilidad internacionales en el entorno digital. Con este fin, han consolidado un marco de comportamiento responsable de los Estados en el uso de las TIC que la Asamblea General ha aprobado por consenso en varias resoluciones[1].

Estos grupos de trabajo también han debatido la instauración de un "diálogo institucional periódico" para tratar las cuestiones relativas al uso de las TIC en el contexto de la seguridad internacional.

Se ha señalado que un diálogo de este tipo debería centrarse especialmente en apoyar la aplicación del marco. En particular, el grupo de trabajo de composición abierta sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional (2019-2021) llegó a la conclusión de que el futuro diálogo institucional periódico "debía ser un proceso orientado a la acción que persiguiera objetivos específicos y se basara en los resultados anteriores, y que fuera inclusivo, transparente, centrado en el consenso y basado en los resultados"[2]. Los Estados también señalaron "la utilidad de explorar mecanismos dedicados al seguimiento de la implementación de las normas y reglas acordadas"[3].

[1] Véanse las resoluciones 70/237 y 76/19 de la Asamblea General.
[2] A/75/816, anexo I, párr. 74.
[3] A/75/816, anexo I, párr. 73.

Los Estados observaron asimismo que el marco era de naturaleza acumulativa y evolutiva y que podrían elaborarse normas complementarias con el tiempo. Por otra parte, tomaron nota de la posibilidad de establecer, en el futuro, nuevas obligaciones vinculantes, según el caso[4]. El futuro diálogo institucional periódico debería fomentar la aplicación del marco ya acordado, pero también permitir una posible evolución de dicho marco en el futuro, sobre todo en un contexto de aparición de nuevos retos y amenazas.

En este contexto, la propuesta presentada inicialmente en 2020 por un grupo interregional de Estados de establecer un programa de acción dotaría a la Primera Comisión de un mecanismo institucional permanente que garantizaría el seguimiento de la aplicación del marco ya acordado y permitiría, en su caso, su evolución.

En su informe sobre un programa de acción para promover el comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional (A/78/76), el Secretario General recomendó que los Estados siguieran examinando los posibles principios, alcance, estructura, contenido, funciones y mecanismo de seguimiento de la propuesta de programa de acción bajo los auspicios 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), basándose en las opiniones expresadas en el informe y teniendo en cuenta las consultas regionales y subregionales organizadas por la Oficina de Asuntos de Desarme de conformidad con lo previsto en la resolución 77/37 de la Asamblea General.

Esta contribución es una actualización de la contribución nacional de Francia incluida en el documento A/78/76, que refleja los avances propiciados por la resolución 78/16 de la Asamblea General y los debates en curso en el seno del grupo de trabajo de composición abierta (2021-2025).

## II. Alcance y objetivos

Como mecanismo de la Primera Comisión, el programa de acción abordaría las cuestiones relativas al uso de las TIC en el contexto de la seguridad internacional. Su objetivo principal sería contribuir al mantenimiento de la paz y la seguridad internacionales preservando un entorno de las TIC abierto, seguro, estable, accesible y pacífico.

A tal fin, los objetivos del programa de acción serían los siguientes:

- La cooperación: reducir las tensiones, prevenir los conflictos y favorecer el uso de las TIC con fines pacíficos gracias a un enfoque de cooperación para hacer frente a las amenazas cibernéticas, así como a un diálogo inclusivo entre los Estados y con las partes interesadas.
- La estabilidad: fomentar la estabilidad en el ciberespacio apoyando la aplicación y, en su caso, la evolución del marco de comportamiento responsable de los Estados basado en el derecho internacional, incluido el derecho internacional humanitario y los derechos humanos, las normas de comportamiento responsable de los Estados, las medidas de fomento de la confianza y la creación de capacidad.
- La resiliencia: contribuir a la reducción de la brecha digital y al fortalecimiento de la resiliencia a nivel mundial en lo que respecta a la aplicación del marco de comportamiento responsable de los Estados.

[4] Resolución 76/19 de la Asamblea General, décimo párrafo del preámbulo.

## III. Estructura y contenido

### Estructura institucional

El programa de acción debería basarse en un documento político cuyo objetivo sería, entre otros:

a) Reafirmar el compromiso político de los Estados en favor del marco de comportamiento responsable de los Estados, tal como se afirma en las resoluciones y los informes pertinentes[5]. Este compromiso fundacional tendría en cuenta los resultados aprobados por consenso en 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), por ejemplo, la creación de un directorio mundial e intergubernamental de puntos de contacto, la puesta en marcha de un portal mundial de cooperación o incluso la posibilidad de crear un registro de amenazas. Un futuro programa de acción debería basarse en estas conclusiones aprobadas por consenso[6];

b) Establecer un mecanismo institucional permanente destinado a: i) favorecer la aplicación de este marco, en particular mediante el refuerzo de las capacidades de los Estados en la materia; ii) seguir haciendo evolucionar el marco, si procede; iii) fomentar la cooperación de múltiples partes interesadas en las esferas pertinentes.

El programa de acción, como mecanismo permanente, podría adoptar la siguiente estructura institucional:

- Organización periódica de sesiones plenarias, por ejemplo, de manera anual o semestral (Francia está dispuesta a proseguir los debates sobre la periodicidad óptima de las reuniones del programa de acción, teniendo en cuenta las capacidades de los Estados y la necesidad de que el programa de acción siga el ritmo de la evolución en el entorno de las TIC). Estas reuniones permitirían: a) debatir las amenazas existentes y emergentes; b) prever la aplicación de normas, reglas y principios; c) proseguir los debates sobre la manera en que el derecho internacional se aplica al uso de las TIC y detectar las lagunas potenciales; d) debatir la puesta en práctica de medidas de fomento de la confianza; e) determinar las prioridades en materia de creación de capacidad, incluida la información facilitada voluntariamente; f) determinar las futuras medidas que deban adoptarse y el programa de trabajo de las reuniones entre períodos de sesiones. Las reuniones anuales podrían decidir por consenso la creación de líneas de trabajo técnicas, abiertas al conjunto de los Estados y partes interesadas, que traten puntos específicos (véase más abajo). Se fomentaría la participación de expertos en los ámbitos técnico y jurídico.
- Organización de reuniones entre períodos de sesiones para avanzar en el programa de trabajo acordado en las reuniones anuales. Estas reuniones podrían estructurarse como reuniones o grupos de trabajo técnicos de composición abierta en torno a ejes de trabajo que traten puntos específicos, de acuerdo con las prioridades y los ámbitos de trabajo identificados en las reuniones anuales.

[5] Esto incluye la resolución 76/19 de la Asamblea General, los informes aprobados por consenso de los grupos de expertos gubernamentales de 2010, 2013, 2015 y 2021, el informe de 2021 del grupo de trabajo de composición abierta (2019-2021) y el primer informe anual sobre la marcha de los trabajos del grupo de trabajo de composición abierta (2021-2025). Debería tenerse en cuenta que los futuros resultados alcanzados por consenso en el actual grupo de trabajo enriquecerán este marco acumulativo y evolutivo.

[6] Véase la resolución 77/37 de la Asamblea General, segundo párrafo del preámbulo, y la resolución 78/16 de la Asamblea General, segundo párrafo del preámbulo.

- Organización de conferencias de examen, por ejemplo, cada cuatro años, que permitan evaluar si el marco debe actualizarse y, si procede, hacerlo evolucionar (véase más abajo). Podría crearse una línea de trabajo específica para profundizar en los debates sobre la manera en que el derecho internacional se aplica al uso de las TIC, y para evaluar si existen lagunas en el marco que justifiquen que se desarrolle este último.

**Contenido**

**a) Promoción de la implementación del marco**

El programa de acción fomentaría la presentación de informes voluntarios sobre las medidas adoptadas en el plano nacional para aplicar el marco, ya sea mediante la creación de su propio sistema de comunicación de información o mediante la promoción de los mecanismos existentes (como el modelo de encuesta nacional de implementación del Instituto de las Naciones Unidas de Investigación sobre el Desarme, o incluso los informes nacionales presentados al Secretario General). Estas comunicaciones permitirían determinar las prioridades en materia de aplicación del marco y evaluar las necesidades de creación de capacidad.

En las reuniones anuales del programa de acción se podrían aprobar y actualizar periódicamente recomendaciones concretas sobre la aplicación en el plano nacional. De conformidad con la estructura institucional descrita anteriormente, las reuniones anuales del programa de acción podrían crear reuniones o grupos de trabajo técnicos de composición cuyo objetivo sería hacer progresar los debates sobre aspectos específicos relacionados con la aplicación del marco.

Por ejemplo, durante una reunión anual podría definirse una prioridad temática para la aplicación del marco (aplicación de una norma o de una medida de fomento de la confianza específicas, seguridad de los productos y servicios digitales, protección de la infraestructura crítica, entre otros). Para proceder a nuevos intercambios de opiniones sobre esta cuestión, aportar conocimientos técnicos especializados, discutir mejores prácticas y dificultades, la reunión anual podría decidir crear una línea de trabajo específica, cuyas actividades estarían abiertas a todos los Estados y tendrían lugar en las reuniones entre períodos de sesiones del programa de acción. Las conclusiones y recomendaciones de estas reuniones o grupos de trabajo técnicos de composición abierta se presentarían en la sesión plenaria siguiente.

El programa de acción apoyaría las medidas de creación de capacidad en lo que se refiere a la aplicación del marco, y tendría por objetivo reforzar la cooperación de múltiples partes interesadas en la materia, así como la coordinación de los esfuerzos con las demás iniciativas pertinentes.

- Los Estados podrían estudiar la creación, en el marco de un futuro programa de acción, de un fondo de contribuciones voluntarias para financiar determinadas actividades destinadas a promover el marco de comportamiento responsable de los Estados. Un fondo de este tipo podría inspirarse en el ejemplo del Servicio Fiduciario de las Naciones Unidas de Apoyo a la Cooperación para la Regulación de los Armamentos[7]. Las iniciativas o los proyectos financiados por este instrumento deberían ajustarse a un mandato, que podría definirse en la primera reunión del programa de acción (promoción de la adhesión al marco, respeto de los principios rectores en materia de creación de capacidad acordados

[7] Servicio Fiduciario de las Naciones Unidas de Apoyo a la Cooperación para la Regulación de los Armamentos, en https://disarmament.unoda.org/unscar/.

en el informe final del grupo de trabajo de composición abierta (2019-2021), entre otros).

- El programa de acción también tendría como objetivo impulsar las acciones e iniciativas existentes. Las reuniones del programa de acción y las reuniones entre períodos de sesiones de un grupo de trabajo técnico sobre la creación de capacidad permitirían a los Estados intercambiar opiniones sobre las prioridades en este ámbito (teniendo en cuenta las necesidades detectadas gracias a la presentación de informes voluntarios), y a las partes interesadas presentar las iniciativas pertinentes. El programa de acción también podría elaborar un sistema de "certificación" para respaldar y promover las actividades que se ajusten a sus objetivos.
- Los representantes de otras organizaciones (Unión Internacional de Telecomunicaciones, Fondo Fiduciario de Donantes Múltiples del Banco Mundial para la Ciberseguridad) podrían realizar presentaciones en las reuniones del programa de acción a fin de garantizar la coordinación y la complementariedad entre las medidas de creación de capacidad adoptadas por las distintas estructuras (cada una en el marco de sus respectivos mandatos y esferas de competencia).

**b) Evolución del marco**

A fin de hacer frente a los nuevos desafíos, las reuniones periódicas o las conferencias de examen, si procede, permitirían actualizar el marco (favoreciendo debates sobre el ulterior desarrollo del marco, entre otras cosas profundizando la comprensión común de las normas y de la aplicación del derecho internacional vigente al uso de las tecnologías de la información y las comunicaciones, señalando las lagunas que mermen dicha comprensión y, si procede, sopesando la necesidad de más normas voluntarias y no vinculantes o de otras obligaciones jurídicamente vinculantes[8]), sobre la base del consenso.

**c) Participación de múltiples partes interesadas**

Francia es consciente de que "los Estados tienen la responsabilidad primordial de mantener la paz y la seguridad internacionales"[9] y de que deben conservar su papel central (incluido el ejercicio exclusivo del poder de decisión) en todos los procesos en el marco de la Primera Comisión, por ello, aboga por un diálogo y una cooperación mayores con las partes interesadas en el marco de un futuro programa de acción.

- La toma de decisiones y la negociación de documentos finales serían competencia exclusiva de los Estados.
- Sin embargo, los grupos de trabajo correspondientes de la Primera Comisión subrayaron en varias ocasiones la necesidad de reforzar aún más la cooperación con la sociedad civil, el sector privado, las universidades y la comunidad técnica[10]. La cooperación con estos actores puede resultar esencial para el cumplimiento por parte de los Estados de sus compromisos en el marco de comportamiento responsable. Además, las partes interesadas tienen "la responsabilidad de utilizar las TIC de forma que no se ponga en peligro la paz y la seguridad"[11]. Los actores privados también pueden aportar una experiencia valiosa a los debates y contribuir a los esfuerzos de creación de capacidad.

[8] Véase la resolución 78/16 de la Asamblea General, tercer párrafo del preámbulo, apartado b).
[9] A/75/816, anexo I, párr. 10.
[10] A/75/816, anexo I, párr. 22.
[11] A/75/816, anexo I, párr. 10.

- Las modalidades de organización de las reuniones del programa de acción deberían permitir a las partes interesadas participar en los períodos de sesiones oficiales, hacer declaraciones y presentar contribuciones, como ocurre en otros procesos pertinentes de la Primera Comisión en los que su experiencia es útil, como el Grupo de Expertos Gubernamentales sobre las Tecnologías Emergentes en el Ámbito de los Sistemas de Armas Autónomos Letales, convocado en el marco de la Convención sobre Prohibiciones o Restricciones del Empleo de Ciertas Armas Convencionales que Puedan Considerarse Excesivamente Nocivas o de Efectos Indiscriminados[12]. Estas modalidades, al permitir el mantenimiento de un diálogo de múltiples partes interesadas en un marco oficial, favorecerían una mayor transparencia del proceso.
- Para garantizar el carácter inclusivo de estas reuniones, debe fomentarse y apoyarse la participación de las partes interesadas de cada grupo regional, en particular mediante programas de patrocinio específicos.

## IV. Modalidades y preparativos relativos al establecimiento de un programa de acción

### Preparativos

Francia es favorable a la continuación de los debates centrados y específicos en el marco del grupo de trabajo de composición abierta (2021-2025) para continuar la elaboración del programa de acción y buscar un consenso en lo que se refiere a su creación.

Los informes finales del grupo de trabajo de composición abierta (2019-2021) y del Grupo de expertos gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional recomendaron que se siguiera elaborando el programa de acción, en particular en el marco del grupo de trabajo de composición abierta (2021-2025). El informe anual de 2022 sobre los progresos realizados del actual grupo de trabajo de composición abierta (2021-2025) también invitó a celebrar debates específicos sobre el programa de acción.

Las consultas regionales celebradas en 2023 y el informe del Secretario General (A/78/76) han permitido recabar las opiniones de un grupo amplio y diverso de Estados. El informe del Secretario General subraya que la consideración de la propuesta de programa de acción de forma inclusiva y transparente, firmemente basada en acuerdos de consenso previos y en los avances logrados en la Asamblea General, es un esfuerzo que merece la pena. El segundo informe anual sobre los progresos realizados por el grupo de trabajo de composición abierta (2021-2025) permitió proseguir esta labor, y en principio se acordaron los “elementos comunes”[13] sobre los que podría alcanzarse un consenso para llegar, de manera constructiva, a una concepción común del futuro mecanismo de diálogo institucional periódico.

La resolución 77/37 de la Asamblea General prevé asimismo que el informe del Secretario General sobre el programa de acción se presente a la Asamblea General y sea examinado por el grupo de trabajo de composición abierta (2021-2025) con miras a proseguir los debates. En su resolución 76/16, la Asamblea General insistió en que el grupo de trabajo de composición abierta debería constituir la principal instancia

[12] Véase el artículo 49 del reglamento aplicable a la Convención sobre Prohibiciones o Restricciones del Empleo de Ciertas Armas Convencionales que Puedan Considerarse Excesivamente Nocivas o de Efectos Indiscriminados (aprobado por la Quinta Conferencia de Examen de las Altas Partes Contratantes en la Convención en 2016).

[13] A/78/265, párr. 55.

para elaborar el programa de acción con miras a su aplicación tras publicarse la labor del grupo de trabajo de composición abierta (2021-2025) y no más tarde de 2026.

Por tanto, en 2024 y 2025 se deberían organizar reuniones entre períodos de sesiones y reuniones específicas del grupo de trabajo de composición abierta (2021-2025) para, entre otras cosas, seguir desarrollando los distintos aspectos del programa de acción y redactar su texto fundacional.

**Establecimiento**

Francia es favorable a la continuación de los debates sobre la forma concreta en que se establecerá el futuro mecanismo.

En su resolución 77/37, la Asamblea General mencionó una "conferencia internacional" como opción para establecer el programa de acción (como ocurrió, en particular, con el Programa de Acción para Prevenir, Combatir y Eliminar el Tráfico Ilícito de Armas Pequeñas y Ligeras en Todos Sus Aspectos). En su resolución 78/16, la Asamblea General decidió crear, bajo los auspicios de las Naciones Unidas, una vez que concluyese la labor del grupo de trabajo de composición abierta (2021-2025) y a más tardar en 2026, un mecanismo permanente, inclusivo y orientado a la acción que tendría los objetivos específicos que se señalaban en su resolución 77/37 y los elementos comunes del futuro diálogo institucional periódico convenidos por consenso en el segundo informe anual sobre la marcha de los trabajos del grupo de trabajo de composición abierta (2021-2025). Si los Estados así lo deciden, en 2025 podría organizarse una conferencia internacional para aprobar el texto fundacional de dicho mecanismo, sobre la base de los trabajos preparatorios realizados en el marco del grupo de trabajo de composición abierta (2021-2025).

Esta conferencia internacional debería tomar sus decisiones por consenso, al menos en lo que se refiere a las cuestiones de fondo. Debería permitir la participación de las partes interesadas (cuya acreditación podría hacerse siguiendo modalidades similares a las adoptadas en la resolución 75/282 de la Asamblea General para el Comité Especial encargado de Elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos).

La Asamblea General podría aprobar una resolución en la que se acogerían favorablemente los resultados de la conferencia y decidiría organizar la primera reunión del nuevo mecanismo.

## Georgia

[Original: inglés
20 de marzo de 2024]

En cuanto al futuro diálogo institucional periódico sobre el uso de las tecnologías de la información y las comunicaciones bajo los auspicios de las Naciones Unidas: Georgia considera que el programa de acción para promover el comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional es el enfoque óptimo para impulsar las iniciativas de las Naciones Unidas en materia de ciberseguridad y comportamiento responsable de los Estados en el ciberespacio.

En un entorno de seguridad como el actual, en el que la evolución geopolítica es impredecible y rápida, algunos agentes ponen en peligro el orden internacional basado en normas utilizando una combinación de métodos de guerra convencionales

y no convencionales. Lamentablemente, hay casos en los que algunos agentes infringen el derecho internacional a través de ciberoperaciones.

La comunidad mundial debe seguir haciendo responsables a dichos agentes de su conducta ilícita e inaceptable en el ciberespacio, y garantizar que dichas acciones tengan consecuencias legales.

El programa de acción podría funcionar como una plataforma adecuada para diálogos específicos sobre la aplicación del derecho internacional en el ciberespacio tras la culminación en 2025 de la labor del actual grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025).

Abogamos por que el programa de acción sirva de marco unificado dentro de la Primera Comisión para afrontar los problemas de ciberseguridad, proporcionando una estructura fiable que propicie iniciativas orientadas a la acción y avances tangibles.

La ausencia de capacidades a escala nacional, regional y mundial supone un reto importante. Por lo tanto, el programa de acción debe complementar las iniciativas nacionales para promulgar el marco normativo y ofrecer asistencia para la creación de capacidad con el fin de reducir la brecha digital.

Georgia acoge con satisfacción la creación de un directorio de puntos de contacto mundial e intergubernamental. Esta iniciativa supone un importante paso adelante en la mejora de la cooperación y la coordinación internacionales en el ámbito de la ciberseguridad en el contexto de las Naciones Unidas.

Dado el rápido ritmo de evolución de las tecnologías de la información y las comunicaciones, el futuro marco internacional debe poseer una amplia flexibilidad para garantizar su pertinencia futura. Este foro internacional debe incorporar un mecanismo que permita el examen periódico de su marco a través del consenso, facilitado por sesiones plenarias periódicas o conferencias de examen. Estas reuniones podrían reevaluar el marco existente y, en su caso, decidir mejorarlo o desarrollarlo.

Georgia apoya firmemente el enfoque transparente e integrador de múltiples partes interesadas, y hace hincapié en la participación activa de los agentes estatales y no estatales en el marco del diálogo institucional sobre estas cuestiones.

## Irlanda

[Original: inglés
1 de mayo de 2024]

Como sociedad abierta con una economía altamente interconectada y digitalizada, Irlanda es plenamente consciente del deterioro de las condiciones seguridad internacionales, especialmente en lo que respecta al aumento de las ciberactividades malintencionadas. Conscientes de ello, hemos tomado medidas a nivel nacional, y con nuestros socios de la Unión Europea, para aumentar la capacidad de reacción, reforzar nuestra capacidad de detectar, prever y neutralizar amenazas, y promover un ciberespacio mundial, abierto y seguro, cuyo núcleo sea el derecho internacional y los derechos humanos.

Sin embargo, hemos sido inequívocos en nuestra postura de que la naturaleza mundial del desafío requiere una respuesta internacional integral. Irlanda apoyó el desarrollo consensuado del marco normativo de las Naciones Unidas de comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones (TIC) y se sintió alentada por dicho desarrollo. El

marco fue un producto crucial de múltiples recomendaciones por consenso tanto de los Grupos de Expertos Gubernamentales (2010, 2013, 2015 y 2021) como del grupo de trabajo de composición abierta sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional (2021). Los dos últimos informes anuales consensuados 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) también respaldaron el marco.

El año pasado, Irlanda publicó su posición nacional de apoyo a la aplicación del derecho internacional en el ciberespacio, uno de los cuatro pilares del marco normativo. Irlanda se compromete a trabajar con otros Estados miembros de la Unión Europea y asociados internacionales para actuar de acuerdo con el marco normativo y promover la paz y la estabilidad mediante su aplicación a escala mundial.

Irlanda considera que la aplicación y la mejora del marco normativo son esenciales para el mantenimiento de la seguridad internacional en el ciberespacio y, por lo tanto, deben ocupar un lugar central en cualquier mecanismo de diálogo institucional periódico. El futuro marco propuesto para el diálogo institucional periódico que puede suceder al actual grupo de trabajo de composición abierta, tal como se prevé específicamente en las propuestas de programa de acción, reconoce que el marco normativo es esencial y permite la celebración de conferencias periódicas de examen para examinar el marco.

Irlanda ha dado siempre su pleno apoyo al enfoque particular del diálogo institucional periódico para la seguridad de las TIC propugnado por el programa de acción, que propone un mecanismo inclusivo y orientado a la acción para un futuro diálogo permanente. El enfoque del programa de acción proporcionaría un diálogo permanente, regionalmente inclusivo, con múltiples partes interesadas y transparente, bajo los auspicios de las Naciones Unidas. El apoyo generalizado al programa de acción, tal como se establece en las resoluciones de la Primera Comisión de la Asamblea General, se ha puesto de manifiesto de forma constante, tanto durante las deliberaciones del grupo de trabajo de composición abierta como a través de los votos de un grupo amplio y regionalmente diverso de Estados en la Asamblea.

Garantizar que todos los Estados puedan aprovechar los beneficios de las TIC, mitigando al mismo tiempo los riesgos mediante medidas de creación de capacidad, es un pilar clave del marco normativo, y una prioridad para Irlanda. Corresponde a los Estados reducir las brechas digitales y reforzar la resiliencia frente a las ciberactividades malintencionadas.

La resolución 78/237 de la Primera Comisión, titulada “Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional”, no refleja la importancia del marco normativo ni la amplia variedad de perspectivas expresadas por muchos Estados Miembros, por lo que Irlanda no ha podido apoyarla. Irlanda no cree que el enfoque propuesto en esta resolución pueda satisfacer las necesidades de la mayoría de los Estados Miembros. De hecho, Irlanda ha llegado a la conclusión de que la resolución puede servir para socavar el método gradual y basado en el consenso a través del cual el grupo de trabajo de composición abierta ha podido avanzar en los últimos años.

Irlanda mantiene la esperanza de que se establezca por consenso un futuro mecanismo de diálogo institucional periódico antes de que finalice la labor del actual grupo de trabajo de composición abierta, y trabajará con todos los Estados para promover un modelo inclusivo y orientado a la acción que refleje el marco normativo.

Los debates sobre cómo podría organizarse el enfoque del programa de acción en particular han incluido propuestas de períodos de sesiones oficiales anuales, con

debates detallados abiertos y reuniones técnicas sobre cuestiones políticas específicas a lo largo del año. Los grupos técnicos podrían abordar cuestiones como el género, las brechas digitales y el papel de las entidades no gubernamentales en la aplicación del marco normativo. Las líneas de trabajo técnicas deben ser voluntarias, estar abiertas a todos los Estados y dar lugar a conclusiones operacionales basadas en las enseñanzas extraídas de la aplicación del marco normativo.

Basándose en el apoyo transregional a las resoluciones de la Primera Comisión que han abogado por un enfoque basado en programas de acción, este mecanismo concreto podría mejorar la participación regional y la cooperación con las organizaciones regionales para apoyar la creación de capacidad en función de las necesidades.

Resulta alentador que el programa de acción propuesto permita también la participación oficial y la celebración de consultas periódicas con las partes interesadas, incluidos el sector privado, el mundo académico y la sociedad civil, para que hagan su contribución sobre las cuestiones pertinentes. Irlanda es firme partidaria de la participación de múltiples partes interesadas en el diálogo institucional periódico, pues cree firmemente que así se centrarán mejor los esfuerzos en ayudar a los Estados a aplicar el marco de comportamiento responsable de los Estados y crear capacidades en función de las necesidades para aumentar la ciberresiliencia.

Con el fin de contar con un diálogo institucional periódico plenamente operativo para el final del mandato del grupo de trabajo de composición abierta, Irlanda apoya la organización de reuniones entre períodos de sesiones y reuniones específicas del grupo de trabajo de composición abierta en 2024 y 2025, en particular sobre las consecuencias presupuestarias.

## Japón

[Original: inglés
30 de abril de 2024]

### 1. Introducción

El Japón apoya la creación de un programa de acción para promover el comportamiento responsable de los Estados en el ciberespacio como futuro mecanismo. El Japón cree que el programa de acción es el foro adecuado para la continuación de nuestros debates sobre el comportamiento responsable de los Estados en el ciberespacio. El programa de acción, como marco orientado a la acción, debería servir de plataforma para apoyar las medidas de cada país para aplicar las normas y principios acordados de comportamiento responsable de los Estados, fomentando el intercambio de mejores prácticas y evaluando los retos específicos a los que se enfrenta cada país.

El programa de acción será el único mecanismo de seguimiento del actual grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025) y entrará en funcionamiento para aplicar los resultados del grupo de trabajo de composición abierta una vez concluido su mandato. El programa de acción se establecerá una vez finalizado el mandato del actual grupo de trabajo de composición abierta y no será de doble vía.

El Japón desearía hacer las mejores contribuciones posibles a los debates, teniendo en cuenta que es de esperar que el programa de acción sirva de formato para la aplicación real de las normas y los principios acordados internacionalmente.

Esta contribución es una actualización de la contribución nacional del Japón incluida en el informe A/78/76 para tener en cuenta el avance propiciado por la resolución 78/16 de la Asamblea General y la continuación de los debates dentro del grupo de trabajo de composición abierta 2021-2025.

## 2. Alcance y objetivos

El propósito del programa de acción es contribuir a mantener la paz y la estabilidad y a promover un entorno de tecnologías de la información y las comunicaciones abierto, seguro, estable, accesible y pacífico.

Con ese fin, el programa de acción debería, en particular, tratar de alcanzar los siguientes objetivos:

a) Formular recomendaciones para orientar los esfuerzos nacionales de aplicación de las normas y los principios de comportamiento responsable de los Estados;

b) Fomentar la presentación de informes voluntarios sobre las prácticas nacionales para determinar las necesidades y los retos de cada Estado Miembro;

c) Apoyar la creación de capacidad, adaptada a las necesidades y los retos, y solicitada por los países beneficiarios;

d) Ser inclusivo y garantizar una amplia participación de los Estados Miembros y de las múltiples partes interesadas.

Además, el programa de acción constituirá una plataforma permanente para avanzar en los temas recurrentes facilitando los debates sobre las amenazas existentes y emergentes, sobre la elaboración de medidas de fomento de la confianza y sobre la manera en que el derecho internacional se aplica al ciberespacio.

## 3. Estructura y contenido

### a) Estructura para promover la aplicación del marco

Para especificar el alcance, la estructura y el contenido del programa de acción, puede utilizarse como referencia los trabajos del Programa de Acción para Prevenir, Combatir y Eliminar el Tráfico Ilícito de Armas Pequeñas y Ligeras en Todos Sus Aspectos. Este programa prevé medidas específicas en los planos nacional, regional e internacional. Cada país presenta un informe voluntario sobre su desarrollo jurídico e institucional y otras prácticas, y celebra una reunión anual de examen.

En el caso del programa de acción sobre cuestiones cibernéticas, el informe voluntario debería incluir una lista de verificación sobre el estado de aplicación de las normas en cada país, como el estado de los esfuerzos para desarrollar políticas, leyes y directrices para la protección de infraestructura crítica y el estado de la respuesta a incidentes en cada país o región. Sería útil que cada Estado Miembro también especificara e incluyera el tipo de creación de capacidad que se necesita. Este ejercicio debería facilitar la creación de un marco de apoyo a las actividades nacionales para aplicar las normas en cada país.

La estructura y las modalidades del programa de acción deberían incluir sesiones plenarias periódicas una o dos veces al año, que se celebrarían en las Naciones Unidas. Las sesiones plenarias del programa de acción podrían adoptar, y actualizar periódicamente, recomendaciones prácticas para las iniciativas nacionales de aplicación. Por ejemplo, las sesiones plenarias pueden determinar una prioridad temática para la implementación del marco, como la aplicación de una norma determinada, las amenazas existentes y emergentes y la protección de infraestructura crítica, entre otros.

Para apoyar nuevos intercambios sobre este tema, las sesiones plenarias pueden decidir crear líneas de trabajo específicas, o reuniones o grupos de trabajo técnicos de composición abierta, que se desarrollarían entre los períodos de sesiones de las sesiones plenarias del programa de acción y que presentarían sus conclusiones a las siguientes sesiones plenarias.

Para complementar los debates sobre la evolución futura del marco, se convocarían conferencias de examen en el marco del programa de acción con una frecuencia por determinar, con vistas a tener en cuenta la rápida evolución de la tecnología y no resultar onerosas, especialmente para las delegaciones de los países en desarrollo.

El directorio mundial de puntos de contacto, que establecerá el actual grupo de trabajo de composición abierta formaría parte integrante del programa de acción para la aplicación y ulterior elaboración de medidas de fomento de la confianza.

**b) Creación de capacidad**

El programa de acción apoyaría los esfuerzos de creación de capacidad en relación con la aplicación del marco, garantizando la participación de múltiples partes interesadas.

Sería útil que el programa de acción detectara las lagunas en la capacidad de los Estados Miembros para aplicar el marco y aprovechar las iniciativas existentes de creación de capacidad para poder colmarlas.

En las reuniones del programa de acción, los representantes de otras organizaciones (por ejemplo, el Centro de Creación de Capacidad en Ciberseguridad de la Asociación de Naciones de Asia Sudoriental y el Japón, el fondo fiduciario de donantes múltiples para la ciberseguridad del Banco Mundial, y la Unión Internacional de Telecomunicaciones) podrían realizar sesiones informativas para garantizar la coordinación y la complementariedad entre las actividades de creación de capacidad emprendidas por cada estructura.

El programa de acción debe funcionar como una plataforma bajo los auspicios de las Naciones Unidas con el fin de crear sinergias y aprovechar los esfuerzos ya realizados por otras organizaciones regionales, en lugar de llevar a cabo programas de creación de capacidad por sí sola.

**c) Derecho internacional y normas**

En mayo de 2021, el Japón presentó y publicó la posición básica del Gobierno del Japón sobre el derecho internacional aplicable a las ciberoperaciones y reafirma que el derecho internacional vigente, incluida la Carta de las Naciones Unidas en su totalidad, es aplicable a estas operaciones. Expone su postura actual sobre la manera en que se aplica el derecho internacional vigente a las ciberoperaciones, centrando sus opiniones en las cuestiones más importantes y básicas. El Gobierno del Japón espera que el anuncio de una posición básica sobre el derecho internacional aplicable a las ciberoperaciones por los Gobiernos de diversos Estados y la aplicación del derecho internacional en tribunales internacionales y nacionales profundizará el entendimiento común internacional acerca de la manera en que el derecho internacional se aplica a las ciberoperaciones en virtud del programa de acción.

El programa de acción también fomentaría la presentación de informes voluntarios sobre los esfuerzos nacionales de aplicación, ya sea creando su propio sistema de presentación de informes o promoviendo los mecanismos existentes (por ejemplo, la encuesta nacional sobre la implementación de las recomendaciones de las Naciones Unidas sobre el uso responsable de las TIC por los Estados en el contexto

de la seguridad internacional del Instituto de las Naciones Unidas de Investigación sobre el Desarme o los informes nacionales al Secretario General). Estos informes servirían de base para determinar las prioridades en la aplicación del marco y para analizar las necesidades en términos de creación de capacidad.

Las sesiones plenarias del programa de acción podrían debatir la manera de profundizar en la comprensión de la aplicación del derecho internacional en el ciberespacio. También podría crearse una línea de trabajo específica para avanzar en los intercambios sobre la manera en que se aplica el derecho internacional vigente a las ciberoperaciones. Sobre la base del mandato encomendado por los Estados Miembros, la línea de trabajo específica podría emplearse para intercambiar opiniones nacionales y llevar a cabo debates basados en hipótesis. Estas líneas de trabajo específicas pueden centrarse en cuestiones generales, conceptos concretos del derecho internacional o temas específicos, como las ciberoperaciones contra infraestructuras críticas, y abarcar al mismo tiempo los principios pertinentes del derecho internacional.

**d) Participación de múltiples partes interesadas**

Las partes interesadas están en el núcleo del ciberespacio, ya sea como propietarios y operadores de elementos de la infraestructura o como voz de las comunidades. Dada la naturaleza interconectada del ciberespacio, es esencial involucrar a la comunidad de múltiples partes interesadas en el debate de las Naciones Unidas.

El programa de acción facilitaría la cooperación y la colaboración con la comunidad de múltiples partes interesadas, en particular para permitir las actividades de creación de capacidad más óptimas posibles.

**4. Preparativos y modalidades para el establecimiento del futuro mecanismo**

El Japón apoya la celebración de nuevos debates específicos en el grupo de trabajo de composición abierta 2021-2025 para seguir elaborando el futuro mecanismo.

## Letonia

[Original: inglés
30 de abril de 2024]

El marco de comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones (TIC) figura desde hace tiempo (desde 2003) en el programa de la Primera Comisión de la Asamblea General y se ha debatido en varios Grupos de Expertos Gubernamentales, así como en grupos de trabajo de composición abierta, lo que pone de relieve la creciente importancia del uso responsable de las TIC para mantener la estabilidad y la seguridad internacionales. La cooperación entre los Estados es vital para hacer frente con eficacia a las crecientes amenazas en el ciberespacio y para fomentar la confianza entre los Estados. Por estas razones, ha llegado el momento de tomar una decisión sobre la creación de un mecanismo permanente en el seno de las Naciones Unidas para abordar las cuestiones de ciberseguridad a largo plazo.

Los ciberataques son cada vez más complejos, destructivos y frecuentes en el mundo moderno interconectado. El panorama cibernético evoluciona constantemente. Aumentan los ciberataques contra infraestructuras críticas, los ataques por motivos políticos, los ataques de *ransomware* y el uso malintencionado de la inteligencia

artificial (IA). La importancia de la ciberseguridad es, por tanto, innegable en el debate internacional sobre seguridad.

Para hacer frente al nivel sin precedentes de actividad malintencionada en el ciberespacio, Letonia está aumentando su propia ciberseguridad y resiliencia. Entre otras cosas, Letonia organiza y lleva a cabo operaciones de caza de ciberamenazas tanto a escala nacional como dentro de la Unión Europea, y nuestras instituciones gubernamentales comparten conocimientos y experiencia con los ciudadanos y las entidades públicas y privadas. En 2023 y 2024, Letonia, junto con otros Estados miembros de la Unión Europea, condenó públicamente en repetidas ocasiones las ciberactividades malintencionadas, incluidos los ciberataques dirigidos contra procesos e instituciones democráticos.

La propuesta de establecer un "diálogo institucional periódico" bajo los auspicios de las Naciones Unidas se ha debatido previamente en la Primera Comisión y se recoge en el informe final del grupo de trabajo de composición abierta 2019-2021[1]. El grupo de trabajo de composición abierta 2019-2021 llegó a la conclusión de que cualquier futuro mecanismo para el diálogo institucional periódico debía ser "un proceso orientado a la acción que persiguiera objetivos específicos y se basara en los resultados anteriores, y que fuera inclusivo, transparente, centrado en el consenso y basado en los resultados"[2]. En el informe anual de 2023 sobre la marcha de los trabajos del grupo de trabajo de composición abierta 2021-2025, los Estados acordaron elementos comunes, sobre todo, un mecanismo permanente de vía única dirigido por los Estados[3].

Las crecientes ciberamenazas exigen que la energía y los recursos de los Estados se centren en mejorar la cooperación y la confianza entre ellos a largo plazo, en lugar de en debates sobre las modalidades de un nuevo mecanismo que se celebran cada pocos años y que suponen un riesgo de fragmentación de los futuros avances. Letonia, como Estado pequeño, apoya un enfoque de vía única que facilitaría el uso eficaz de unos recursos limitados.

En respuesta a la petición de que se establezca un mecanismo permanente para fomentar el comportamiento responsable de los Estados en el uso de las TIC con un planteamiento coherente y a largo plazo, se ha propuesto un programa de acción[4]. Las resoluciones de la Asamblea General 77/37[5] sobre el programa de acción en 2022 y 78/16[6] sobre el programa de acción en 2023 recibieron un amplio apoyo de los Estados en la Asamblea General, y esta iniciativa se ha desarrollado de forma transparente, inclusiva y gradual.

*El programa de acción como mecanismo permanente de las Naciones Unidas*

Letonia opina que, en virtud de las resoluciones 77/37 y 78/16, la Asamblea General ha otorgado un mandato firme para proceder al establecimiento del programa de acción. El programa de acción debe ser un mecanismo permanente, inclusivo, orientado a la acción y dirigido por los Estados en el seno de la Primera Comisión,

[1] Informe final del grupo de trabajo de composición abierta 2019-2021, párrafos 68 a 74.

[2] *Ibid*., párr. 74.

[3] Segundo informe anual sobre la marcha de los trabajos del grupo de trabajo de composición abierta 2021-2025 (A/78/265), párr. 55 a).

[4] https://documents.unoda.org/wp-content/uploads/2021/11/Working-paper-on-the-proposal-for-a-Cyber-PoA.pdf.

[5] Resolución 77/37 de la Asamblea General, Programa de acción para promover el comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional.

[6] Resolución 78/16 de la Asamblea General, Programa de acción para promover el comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional.

así como una plataforma para la participación de todos los Estados. Su objetivo general sería contribuir al fortalecimiento de la paz y la seguridad internacionales y a la prevención de conflictos y malentendidos entre los Estados. El ámbito del programa de acción deberían ser las cuestiones relacionadas con el uso de las TIC de conformidad con el derecho internacional y la aplicación del marco de las Naciones Unidas de comportamiento responsable de los Estados en el ciberespacio. Como se señala en la resolución 77/37 de la Asamblea General, el programa de acción "tendrá en cuenta los resultados de consenso aprobados"[7] por el grupo de trabajo de composición abierta 2021-2025.

Se promoverían la estabilidad y la seguridad en el ciberespacio apoyando la aplicación, y el desarrollo ulterior, si procede[8], del marco de comportamiento responsable de los Estados basado en el derecho internacional, incluida la Carta de las Naciones Unidas en su totalidad. Como se acordó en los informes del Grupo de Expertos Gubernamentales de 2013, 2015 y 2021 y en los informes del grupo de trabajo de composición abierta de 2021 y 2022, el derecho internacional, incluido el derecho internacional humanitario, es aplicable y esencial para mantener la paz, la seguridad y la estabilidad en el ciberespacio.

Para promover la aplicación del marco de comportamiento responsable de los Estados, el programa de acción apoyaría las actividades pertinentes de creación de capacidad en función de las necesidades. Es importante avanzar en el trabajo colectivo sobre creación de capacidades y compartir nuestra experiencia y mejores prácticas para mejorar la resiliencia tanto nacional como mundial ante las ciberamenazas.

En el marco del programa de acción podrían celebrarse períodos de sesiones oficiales anuales. Entre los períodos de sesiones oficiales, el trabajo del programa de acción podría organizarse en grupos de trabajo técnicos dedicados a temas específicos. Por ejemplo, un grupo de trabajo técnico podría ocuparse mejorar la comprensión de la manera en que se aplica el derecho internacional al uso de las TIC. Las recomendaciones elaboradas por los grupos de trabajo técnicos se adoptarían en los períodos de sesiones oficiales. Las nuevas prioridades del programa de acción deberían revisarse periódicamente durante las conferencias de examen.

Los grupos técnicos podrían crearse y disolverse por decisión de los períodos de sesiones oficiales. Los grupos de trabajo técnicos serían inclusivos y estarían abiertos a todos los Estados que desearan unirse a ellos, y habría que esforzarse por garantizar que los expertos nacionales pudieran participar presencialmente o en línea (formato híbrido). Las decisiones sobre los grupos técnicos y sus modalidades de trabajo deben tomarse teniendo en cuenta la capacidad y los recursos de los Estados pequeños.

El diálogo regular y completo con las partes interesadas (sociedad civil, sector privado, mundo académico) es esencial y debe facilitarse a través del programa de acción. Su experiencia en el ciberdominio, en constante evolución, es inestimable, por lo que su aportación es importante para avanzar en la aplicación de un comportamiento responsable de los Estados. Las propias partes interesadas también "tienen la responsabilidad de utilizar las TIC de forma que no pongan en peligro la paz y la seguridad"[9], ya que son ellas las que impulsan el desarrollo de las nuevas tecnologías.

En 2024 y 2025 deberían organizarse nuevos debates específicos en los períodos de sesiones restantes y en las reuniones entre períodos de sesiones del grupo de trabajo

[7] Resolución 77/37 de la Asamblea General, segundo párrafo del preámbulo.
[8] Resolución 76/19 de la Asamblea General, décimo párrafo del preámbulo.
[9] Informe final del grupo de trabajo de composición abierta (2019-2021), párr. 10.

de composición abierta (2021-2025) para seguir elaborando los diferentes aspectos del programa de acción, incluidas las modalidades para su establecimiento. El programa de acción debería estar operativo tras la conclusión de la labor del grupo de trabajo de composición abierta (2021-2025).

## Nueva Zelandia

[Original: inglés
30 de abril de 2024]

1. La ciberseguridad es un tema de debate entre los Estados, bajo los auspicios de las Naciones Unidas, desde hace más de 20 años. Sucesivos grupos de trabajo -grupos de expertos gubernamentales y grupos de trabajo de composición abierta- han permitido mantener intercambios periódicos sobre cuestiones relacionadas con la ciberseguridad en el contexto de la seguridad internacional.

2. Estos grupos de trabajo han aportado importantes resultados fundacionales que contribuyen colectivamente a la seguridad y la estabilidad internacionales mediante el establecimiento de un marco de comportamiento responsable de los Estados en el ciberespacio que la Asamblea General de las Naciones Unidas ha hecho suyo y se basa en cuatro pilares:

- Derecho internacional: todos los Estados Miembros de las Naciones Unidas están de acuerdo en que el derecho internacional se aplica al comportamiento de los Estados en el ciberespacio
- Normas de comportamiento responsable de los Estados en línea en tiempos de paz
- Medidas de fomento de la confianza para apoyar la transparencia, la previsibilidad y la estabilidad
- Medidas de creación de capacidad destinadas a garantizar que todos los Estados puedan reducir los riesgos asociados al aumento de la conectividad, sin dejar de beneficiarse de ella

3. Nueva Zelandia respalda plenamente la decisión que tomó la Asamblea General en su resolución 78/237 de crear, bajo los auspicios de las Naciones Unidas, una vez que concluyera la labor del grupo de trabajo de composición abierta (2021-2025) y a más tardar en 2026, un mecanismo permanente, inclusivo y orientado a la acción que tendría los objetivos específicos que se señalaban en su resolución 77/37 y los elementos comunes del futuro diálogo institucional periódico convenidos por consenso en el informe anual del grupo de trabajo de composición abierta (2021-2025) sobre los progresos realizados presentado en 2023.

4. Prevemos que este mecanismo sea el “hogar permanente” de los debates sobre ciberseguridad en el contexto de la seguridad internacional en las Naciones Unidas, al término de la labor del actual grupo de trabajo de composición abierta 2021-2025, y basándose en la propuesta aprobada en las resoluciones 77/37 y 78/237 de las Naciones Unidas. Acogemos con satisfacción y apoyamos la resolución presentada por Francia, en nombre de un grupo interregional, que proporciona una vía clara y transparente para que todos los Estados consideren el ámbito, la estructura, el contenido y las modalidades del futuro mecanismo de forma que complemente al actual grupo de trabajo de composición abierta. A este respecto, apoyamos el establecimiento de un programa de acción que:

a) Sea el único mecanismo permanente para los debates sobre ciberseguridad de las Naciones Unidas después de 2025, garantizando la previsibilidad y la

estabilidad institucional. La negociación de modalidades acordadas para un mecanismo permanente también aportaría eficiencias a largo plazo. Revisar y acordar las modalidades de los sucesivos grupos de trabajo ha exigido largas y repetidas negociaciones, lo que ha restado tiempo a importantes debates de fondo;

b) Esté anclado en el marco acordado de comportamiento responsable de los Estados en el ciberespacio, sea coherente con las obligaciones relativas al derecho internacional y los derechos humanos internacionales, garantizando que el programa de acción se base en el trabajo fundacional de los sucesivos Grupos de Expertos Gubernamentales y grupos de trabajo de composición abierta y mejore dicho trabajo para promover el comportamiento responsable de los Estados en línea;

c) Incluya la participación de múltiples partes interesadas, incluidos los Gobiernos (responsables de la paz y la seguridad internacionales en el ciberespacio), las empresas, la sociedad civil, los expertos técnicos, los académicos y otras organizaciones que contribuyen a una Internet libre, abierta, segura e interoperable. Nueva Zelandia apoya las modalidades que incluyen la participación, incluidas las declaraciones y la presentación de informes escritos, de las partes interesadas no gubernamentales en los debates, incluidas las reuniones oficiales y oficiosas y las conferencias de examen;

d) **Esté orientado a la acción**, con atención a las medidas prácticas para promover el marco de comportamiento responsable de los Estados y fomentar medidas de creación de capacidad que ayuden a los Estados a aplicar el marco y los mecanismos de rendición de cuentas y seguimiento;

e) Sea flexible y adaptable, para responder a las amenazas emergentes.

## Países Bajos (Reino de los)

[Original: inglés
1 de mayo de 2024]

### Introducción

Los Países Bajos siguen profundamente preocupados por el creciente riesgo que supone el uso malintencionado de las tecnologías de la información y las comunicaciones (TIC) por parte de agentes estatales y no estatales para la seguridad y la estabilidad internacionales, el desarrollo económico y social y la seguridad y el bienestar de las personas. También se señala que los diferentes niveles de capacidad de los Estados en materia de seguridad de las TIC pueden hacer aumentar la vulnerabilidad en un mundo cada vez más interconectado.

Para hacer frente a estos retos, los Estados han desarrollado, a través del trabajo de una serie de procesos intergubernamentales, un marco acumulativo y evolutivo de comportamiento responsable de los Estados en el uso de las TIC en el contexto de la seguridad internacional. La Asamblea General ha respaldado repetidamente este marco mediante resoluciones consensuadas.

Para aprovechar estos logros, los Países Bajos subrayan la necesidad de establecer un diálogo institucional periódico tras la conclusión del actual grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025), creado en virtud de la resolución 75/240 de la Asamblea General. En este sentido, los Países Bajos apoyan la iniciativa de establecer un futuro programa de acción para promover el comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional, acogida favorablemente por la Asamblea General en sus resoluciones 77/37 y 78/16.

De conformidad con el párrafo 8 de la resolución 78/237, titulada “Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional”, los Países Bajos presentan por la presente sus opiniones y observaciones sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso, en particular sobre el futuro diálogo periódico sobre esas cuestiones que se celebrará bajo los auspicios de las Naciones Unidas. Las opiniones que se presentan a continuación se basan en la presentación de los Países Bajos para el informe del Secretario General de conformidad con la resolución 77/37 (A/78/76).

Dentro del grupo de trabajo de composición abierta 2021-2025, se ha avanzado considerablemente en la búsqueda de una base común sobre el futuro mecanismo de diálogo institucional periódico sobre la seguridad internacional de las TIC. A este respecto, los Países Bajos acogen con satisfacción los elementos comunes sobre el diálogo institucional periódico contenidos en el informe anual de 2023 sobre la marcha de los trabajos del grupo de trabajo de composición abierta. Los Países Bajos mantienen su compromiso de seguir avanzando en este asunto dentro del grupo de trabajo de composición abierta 2021-2025.

**Ámbito y objetivos**

Reafirmando el párrafo 4 de la resolución 78/16 de la Asamblea General, los Países Bajos opinan que debe crearse, bajo los auspicios de las Naciones Unidas, una vez que concluya la labor del grupo de trabajo de composición abierta (2021-2025) y a más tardar en 2026, un mecanismo permanente, inclusivo y orientado a la acción que tendrá los objetivos específicos que se señalan en la resolución 77/37 de la Asamblea General y los elementos comunes del futuro diálogo institucional periódico convenidos por consenso en el informe anual del grupo de trabajo de composición abierta (2021-2025) sobre los progresos realizados presentado en 2023.

Los Países Bajos apoyan la iniciativa de establecer, bajo los auspicios de las Naciones Unidas, un programa de acción para promover el comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional. El programa de acción debería utilizar los elementos comunes para el futuro diálogo institucional periódico acordados por consenso en el informe anual de 2023 sobre la marcha de los trabajos del grupo de trabajo de composición abierta y basar las decisiones relativas al ámbito, la estructura, el contenido y las modalidades en los resultados consensuados del grupo de trabajo de composición abierta de 2021-2025.

**Estructura y modalidades**

Los Países Bajos comparten la opinión de que el programa de acción debería ser un proceso inclusivo, transparente, basado en el consenso y en los resultados. El mandato del programa de acción podría derivarse de un documento fundacional en el que se afirmara el compromiso político de los Estados de guiarse por el marco de comportamiento responsable de los Estados en el ciberespacio y se estableciera un mecanismo para operacionalizar sus objetivos.

El programa de acción debería estar abierto a la participación de todos los Estados Miembros de las Naciones Unidas, observadores permanentes, organizaciones intergubernamentales y de otra índole y organismos especializados. Aunque los Estados son los principales responsables del mantenimiento de la paz y la seguridad internacionales, el programa de acción también debería permitir la participación significativa, incluso en contextos oficiales, de las partes interesadas no gubernamentales pertinentes, incluidos el sector privado, el mundo académico y la sociedad civil.

La estructura del programa de acción podría abarcar lo siguiente:

a) Conferencias periódicas de examen para evaluar la evolución del panorama de las ciberamenazas y las iniciativas del programa de acción, actualizar el marco en caso necesario y proporcionar orientación estratégica;

b) Debates plenarios abiertos para debatir las amenazas actuales y emergentes, profundizar en el modo en que se aplica el derecho internacional, debatir la aplicación de medidas de fomento de la confianza, determinar las prioridades en materia de desarrollo de capacidades y estudiar la aplicación de normas, reglas y principios, así como para proporcionar orientaciones para las reuniones técnicas abiertas y las iniciativas prácticas;

c) Reuniones o grupos de trabajo técnicos de composición abierta para debates orientados a la acción, abiertos a la participación de las partes interesadas pertinentes y dedicados a cuestiones específicas.

**Preparativos y modalidades para el establecimiento del programa de acción**

La resolución 78/16, la resolución 77/37 y el informe del Secretario General (A/78/76) proporcionan una hoja de ruta inicial para establecer el programa de acción. En 2025-2026, tras concluir la labor del grupo de trabajo de composición abierta, los Países Bajos prevén que se celebre una conferencia internacional, abierta a las partes interesadas no gubernamentales, que se base en los trabajos preparatorios realizados, incluidos los del grupo de trabajo de composición abierta 2021-2025, para aprobar el documento fundacional o la declaración política.

**Creación de capacidad en un futuro mecanismo**

Sin perjuicio de los resultados del grupo de trabajo de composición abierta y de las decisiones de la Asamblea General sobre el establecimiento de un futuro mecanismo, los Países Bajos proponen los siguientes elementos para facilitar la creación de capacidades cibernéticas para avanzar en la aplicación del marco evolutivo y acumulativo y reforzar la cooperación internacional a este respecto. Esta propuesta gira en torno a un ciclo de cuatro etapas:

a) Intercambios sobre el panorama de las amenazas mediante el intercambio de conocimientos técnicos sobre las amenazas y el estudio de cómo hacer frente a estas amenazas a través de la lente del marco consensuado de comportamiento responsable de los Estados en el ciberespacio;

b) La autoidentificación de las necesidades de capacidad mediante la presentación voluntaria de informes en relación con el marco acumulativo y evolutivo de comportamiento responsable de los Estados. Pueden utilizarse los métodos existentes de notificación voluntaria, por ejemplo la encuesta nacional de UNIDIR (iniciativa mexicano-australiana) sobre la implementación de las recomendaciones de las Naciones Unidas sobre el uso responsable de las TIC por los Estados en el contexto de la seguridad internacional;

c) Ajustar recursos y necesidades. El futuro mecanismo podría funcionar como una plataforma de convocatoria. Además, dado el carácter universal y el reconocimiento de las Naciones Unidas, la Secretaría de las Naciones Unidas podría desempeñar un papel a la hora de facilitar la coordinación del trabajo de las organizaciones y estructuras en materia de creación de capacidades cibernéticas. El futuro mecanismo podría basarse en herramientas ya existentes, como el portal Cybil del Foro Mundial de Competencia Cibernética, y, posiblemente, en propuestas actualmente en estudio en el grupo de trabajo de composición abierta 2021-2025, como el catálogo de creación de capacidades y el portal de cooperación mundial en materia de ciberseguridad propuestos por los Estados Miembros;

d) Un bucle de retroalimentación mediante el cual los Estados podrían intercambiar experiencias en sus esfuerzos de implementación y actividades de creación de capacidades cibernéticas, que podrían informar futuros debates sobre el uso de las TIC por parte de los Estados en el contexto de la seguridad internacional.

Los esfuerzos de creación de capacidad como parte del futuro mecanismo deben llevarse a cabo de acuerdo con los principios para la creación de capacidad acordados en el informe anual de 2023 sobre la marcha de los trabajos del grupo de trabajo de composición abierta.

## Singapur

[Original: inglés
1 de mayo de 2024]

Singapur sigue comprometido con una conversación global abierta e inclusiva sobre ciberseguridad, y es en este sentido que consideramos de suma importancia el compromiso de todos los Estados con un futuro diálogo institucional periódico de una sola vía. Un futuro diálogo institucional periódico de una sola vía es crucial para fomentar la aceptación y el reconocimiento universales del marco acumulativo y evolutivo de comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones (TIC) acordado por todos los Estados Miembros en las Naciones Unidas desde 1998, y para proporcionar una plataforma global común para el desarrollo y la aplicación ulteriores de este marco. En este sentido, es importante que todos los Estados puedan centrar sus esfuerzos en un único proceso para garantizar que los debates sigan siendo sustantivos y no sufran fragmentación. Los Estados pequeños y en desarrollo con recursos limitados tampoco podrían participar de forma sostenible en procesos paralelos de doble vía.

Singapur cree que debemos seguir basándonos en los cuatro elementos comunes del diálogo institucional periódico acordado en el segundo informe anual sobre la marcha de los trabajos del grupo de trabajo de composición abierta sobre la seguridad de las TIC y de su uso (2025-2025) (A/78/265, párr. 55) para generar la confianza que necesitamos para llegar a un consenso sobre un mecanismo permanente de vía única.

Es importante que los Estados utilicen el poco tiempo y espacio que les queda para trabajar en la construcción de una visión común sobre el camino a seguir para un diálogo institucional regular dentro del actual grupo de trabajo de composición abierta. La tarea prioritaria debe ser la búsqueda de consenso. En este sentido, Singapur apoya la propuesta formulada por el Brasil en el séptimo período de sesiones sustantivo del grupo de trabajo de composición abierta para que se establezca una moratoria en la presentación de resoluciones relativas a la seguridad de las TIC en la Primera Comisión de la Asamblea General hasta que el actual grupo de trabajo de composición abierta concluya su labor en 2025. Apoyamos a la Presidencia del grupo de trabajo de composición abierta para que siga convocando debates sobre el camino a seguir para un diálogo institucionalizado regular, con vistas a seguir desarrollando y perfeccionando una propuesta consensuada para dicho diálogo.

Como siguiente paso, creemos que sería productivo que el actual grupo de trabajo de composición abierta acordara el alcance, la estructura, los objetivos y la frecuencia de las reuniones del futuro mecanismo. Responder a estas cuestiones prácticas es una forma lógica de partir de los elementos comunes que todos los Estados ya han acordado. De este modo, las delegaciones, en particular las más pequeñas y con recursos limitados, tendrán claro desde el principio cuál será su trabajo después de 2025, lo que les permitirá empezar a planificar lo necesario para optimizar su participación de manera significativa. Para garantizar una base sostenible para un mecanismo universal permanente de vía única, Singapur también

hace hincapié en que el diseño del futuro mecanismo debe ser lo suficientemente amplio y complaciente como para facilitar debates continuos y futuros sobre las propuestas y prioridades de todas las delegaciones. En particular, sería útil examinar periódicamente las operaciones del mecanismo permanente para garantizar que sus enfoques sean pertinentes para el dinámico panorama operativo de las amenazas. En este sentido, Singapur apoya el enfoque y la estructura presentados en el documento de debate de la Presidencia del 20 de febrero de 2024 sobre el proyecto de elementos para el mecanismo permanente. Singapur espera con interés trabajar constructivamente con todas las delegaciones para seguir perfeccionando estos proyectos de elementos con vistas a su adopción por consenso en el tercer informe anual sobre la marcha de los trabajos del actual grupo de trabajo de composición abierta.

## Türkiye

[Original: inglés
1 de mayo de 2024]

Las tecnologías de la información y las comunicaciones se han convertido en una parte indispensable de la sociedad y la economía al afectar a todos los aspectos de la vida. Estas tecnologías son utilizadas en muchos ámbitos tanto por particulares como por Estados. Hoy en día, las capacidades de los Estados para desarrollar y utilizar la tecnología desempeñan un papel importante en el desarrollo y el crecimiento. Las tecnologías de la información se han convertido en el principal protagonista del desarrollo en casi todos los campos, del transporte a las comunicaciones, de la industria de defensa a la ciencia médica, y de la producción a la educación y el comercio.

Los estudios indican que las tendencias tecnológicas se acelerarán en los próximos años. Entre ellas, destacan las que pueden aportar nuevos estándares tecnológicos y nuevas líneas de negocio e introducir cambios significativos en las ya existentes. La Internet de los objetos, la conexión 5G, los macrodatos, la tecnología de cadenas de bloques, la inteligencia artificial, los vehículos autónomos y los robots inteligentes se consideran tecnologías que arrojarán luz sobre nuestro presente y nuestro futuro.

Por otra parte, aunque estas tecnologías nos brindan muchas oportunidades, también conllevan riesgos de ciberseguridad. Las estructuras de las ciberamenazas son cada vez más complejas y su número aumenta día a día y, según las investigaciones, se ha determinado que habrá más de 493 millones de intentos de *ransomware* en todo el mundo en 2022[1].

En este sentido, la ciberseguridad es una necesidad que debe abordarse en todas las etapas para el sano desarrollo e integración de la tecnología. Las vulnerabilidades de seguridad en los sistemas de información y comunicaciones pueden provocar que estos sistemas queden fuera de servicio o sean utilizados indebidamente, o causar la pérdida de vidas humanas, daños económicos a gran escala, alteración del orden público o violación de la seguridad nacional.

Garantizar la ciberseguridad no es solo una necesidad para combatir las amenazas en ámbitos donde la tecnología es intensa, sino también un factor importante que afecta al bienestar y la seguridad nacional de los países debido a los riesgos que conlleva para el curso de la vida social y económica. A la luz de todos estos acontecimientos, los países gastan cantidades muy elevadas en el campo de la

[1] www.statista.com/statistics/494947/ransomware-attempts-per-year-worldwide.

ciberseguridad, desarrollan tecnologías de ciberseguridad y dirigen sus esfuerzos a garantizar su seguridad en el ciberentorno y aumentar su resistencia contra los ataques.

La cuestión de la lucha contra las ciberamenazas se considera una política nacional en nuestro país. En este contexto, los estudios para garantizar la ciberseguridad nacional corren a cargo del Ministerio de Transportes e Infraestructuras a nivel estratégico y de la Autoridad de Tecnologías de la Información y las Comunicaciones (BTK) a nivel técnico. Además, otras instituciones y organizaciones también contribuyen a estos estudios.

En el marco de los estudios llevados a cabo desde 2012, se han elaborado y aplicado la "Estrategia Nacional de Ciberseguridad y los Planes de Acción". Más recientemente, de acuerdo con la "Estrategia Nacional de Ciberseguridad y Plan de Acción (2020-2023)", se han llevado a cabo estudios para proteger la ciberseguridad de las infraestructuras críticas 24 horas al día, 7 días a la semana, aumentar las competencias de los equipos de respuesta a ciberincidentes y el uso seguro del ciberespacio por parte de todos los segmentos de la sociedad, mantener la concienciación sobre la ciberseguridad a un alto nivel, compartir información y cooperación con las partes interesadas nacionales e internacionales, desarrollar mecanismos que garanticen la protección, minimizar los ciberdelitos y aumentar la disuasión.

Además, el Ministerio de Transportes e Infraestructuras ha iniciado estudios para elaborar una nueva estrategia y plan de acción de ciberseguridad que abarque el período 2024-2028. En este contexto, prosiguen los estudios para garantizar una cooperación eficaz entre todas las partes interesadas, aumentar la adquisición, producción e intercambio de información sobre amenazas a la ciberseguridad, incrementar el nivel de preparación nacional ante ciberincidentes, desarrollar recursos humanos expertos, desarrollar oportunidades de detección rápida y respuesta temprana y realizar análisis de riesgos para sectores e infraestructuras críticos.

El TR-CERT (Equipo Nacional de Respuesta a Emergencias Cibernéticas de Türkiye, que forma parte de la Autoridad de Tecnologías de la Información y las Comunicaciones), ha coordinado la respuesta a incidentes cibernéticos en Türkiye desde 2013. Además de la detección de ciberamenazas y la respuesta a ciberincidentes, incluidos el antes, el durante y el después de los incidentes, el TR-CERT garantiza la aplicación de medidas preventivas contra las ciberamenazas y se asegura de disuadir a los ciberdelincuentes.

Las principales áreas de interés en ciberseguridad del TR-CERT son:

- Creación de cibercapacidad
- Medidas tecnológicas
- Recopilación y difusión de información sobre amenazas
- Protección de la infraestructura crítica

En el contexto de la mejora de la ciberseguridad nacional, desde 2013 también se han creado 14 equipos sectoriales de respuesta a emergencias cibernéticas para sectores o infraestructuras críticos (como la energía, la sanidad, la banca y las finanzas, la gestión hídrica, las comunicaciones electrónicas y los servicios públicos críticos) y más de 2.200 equipos institucionales de respuesta a emergencias cibernéticas. Todos los equipos de respuesta a emergencias cibernéticas trabajan 24 horas al día, 7 días a la semana, bajo la coordinación del TR-CERT para mitigar los ciberriesgos y luchar contra las ciberamenazas. El TR-CERT utiliza herramientas de detección y prevención para la supervisión, y herramientas de notificación para

compartir información con las partes pertinentes. El TR-CERT ha desarrollado una plataforma de intercambio de información para todos los equipos de respuesta de emergencias cibernéticas de Türkiye con el fin de distribuir alarmas, avisos y notificaciones de seguridad, lo que proporciona un canal de comunicación eficaz y seguro.

Los ejercicios de ciberseguridad son otra actividad importante para la cooperación y la preparación. Este tipo de ejercicios realizados a nivel nacional e internacional contribuyen al fortalecimiento del ciberespacio y al ensayo de las medidas a adoptar frente a posibles ciberamenazas. Desde 2011, el Ministerio de Transportes e Infraestructuras ha organizado siete ejercicios de ciberseguridad nacionales y dos internacionales. Recientemente, a escala nacional, se han llevado a cabo los ejercicios "Cyber Shield 2022". Después de Cyber Shield 2022, con la cooperación de nuestro Ministerio de Transporte e Infraestructuras y la Autoridad de Tecnologías de la Información y las Comunicaciones (BTK), se celebró "Cyber Shield 2022 para el sector financiero" los días 20 y 21 de octubre de 2022 con la participación de instituciones y organizaciones públicas. En estos ejercicios, con la infraestructura técnica y los escenarios desarrollados en el seno del TR-CERT, se proporcionó a los participantes experiencia práctica en ciberseguridad y se compartió información sobre los pasos a seguir en caso de posibles ciberataques. Está previsto organizar un ejercicio internacional de ciberseguridad en el próximo período.

La ciberseguridad es una cuestión que está en la agenda de todo el mundo y requiere esfuerzos a escala internacional. La cooperación a escala regional y mundial y el intercambio de información e inteligencia en el ámbito de la ciberseguridad desempeñan un papel importante para ayudar a los países a hacer frente a los ciberriesgos y las amenazas. En este contexto, Türkiye está desarrollando la cooperación bilateral, regional e internacional en este campo; participa y contribuye a las actividades de elaboración de políticas y estrategias de organizaciones internacionales como las Naciones Unidas, la Organización del Tratado del Atlántico Norte (OTAN), la Organización para la Seguridad y la Cooperación en Europa (OSCE), el G20, la Organización de Cooperación y Desarrollo Económicos, la Organización de Cooperación Económica, el D8, el Centro de Cooperación en materia de Seguridad (RACVIAC), la Organización de Estados Turcos, etc. Además, el TR-CERT prosigue sus actividades de intercambio de información sobre ciberamenazas a través de su pertenencia a plataformas internacionales como el Foro de Equipos de Respuesta a Incidentes y Seguridad (FIRST), TI, la UIT, la Alianza de Ciberseguridad para el Progreso Mutuo, la Plataforma de Intercambio de Información sobre Malware de la OTAN y el Equipo de Respuesta a Emergencias Informáticas de la Organización de Cooperación Islámica (OIC-CERT). Nuestro país también participa en el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (NATO CCDCoE) como país patrocinador y es miembro del mecanismo de Capacidad Virtual de Apoyo a Incidentes Cibernéticos (VCISC) de la OTAN. Además, se firman memorandos de entendimiento y cooperación bilateral con muchos países en materia de ciberseguridad.

El TR-CERT ha sido aceptado en el programa Common Vulnerabilities and Exposures (MITRE-CVE) y, en este contexto, asigna números CVE para las vulnerabilidades del software, el hardware o los productos de terceros y proporciona coordinación de procesos en la gestión de vulnerabilidades.

Türkiye es parte en varios acuerdos multilaterales sobre ciberseguridad. Türkiye ratificó el Convenio sobre la Ciberdelincuencia (*European Treaty Series* núm. 185) del Consejo de Europa. Türkiye también ha contribuido a los estudios realizados en el marco del Comité Especial de las Naciones Unidas encargado de Elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos. Además, Türkiye es uno de los Estados copatrocinadores del programa de acción para

promover un comportamiento responsable de los Estados en la utilización de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional y apoya firmemente la resolución 77/37 de la Asamblea General de las Naciones Unidas y los esfuerzos ulteriores para el establecimiento del programa de acción como mecanismo permanente, inclusivo y orientado a la acción.

### 1. Organización Nacional de Ciberseguridad de Türkiye

Si nos fijamos en el ámbito de la seguridad de la información y las comunicaciones, en particular la ciberseguridad en Türkiye, cabe destacar que la progresión en este campo se remonta a 1991. La andadura de Türkiye en materia de ciberseguridad comenzó con la introducción de los ciberdelitos en la Ley Penal de Türkiye núm. 765 en 1991[2]. Desde entonces, ha logrado importantes hitos en diversos ámbitos de la ciberseguridad, parte esencial de la seguridad nacional. A continuación figura una lista no exhaustiva de las iniciativas aplicadas hasta 2012:

- El Plan Maestro Nacional de Infraestructuras de la Información[3] se elaboró en Türkiye en 1999.
- El Plan de Acción de la Iniciativa E-Türkiye[4] se puso en marcha en 2002.
- El proyecto E-Transformation Türkiye se esbozó en 2003 junto con el Plan de Acción a Corto Plazo para 2003-2004[5].
- La introducción de la Ley de Firma Electrónica núm. 5070[6] y la Ley del Código Penal de Türkiye núm. 5237[7] en 2004.
- La publicación de la Estrategia y Plan de Acción de la Sociedad de la Información[8] 2006-2010 en 2006.
- La creación del Centro de Coordinación del Equipo Turco de Respuesta a Incidentes Informáticos en 2007.
- En 2007 se promulgó la Ley núm. 5651, sobre publicaciones en Internet y lucha contra los delitos cometidos por medio de dichas publicaciones[9].
- La Ley de Comunicaciones Electrónicas núm. 5809[10] se promulgó en 2008, coincidiendo con el primer Simulacro Nacional de Ciberseguridad.
- En 2010 se publica la Declaración del Consejo de Seguridad Nacional, en la que se reconoce el alcance mundial de las ciberamenazas y sus implicaciones para la seguridad nacional.
- Ese mismo año se logró la adhesión de Türkiye al Convenio de Budapest del Consejo de Europa (CE) sobre la Ciberdelincuencia (*ETS* núm. 185).
- La decisión del Consejo de Ministros de gestionar y coordinar los esfuerzos nacionales de ciberseguridad dio lugar a la creación del Consejo de Ciberseguridad en 2012[11], y el Instituto de Ciberseguridad[12] del Centro de

[2] https://www.mevzuat.gov.tr/MevzuatMetin/5.3.765.pdf.
[3] http://www.bilgitoplumu.gov.tr/Documents/1/Yayinlar/991000_TuenaRapor.pdf.
[4] http://www.bilgitoplumu.gov.tr/Documents/1/Yayinlar/020800_E-TurkiyeEylemPlani.pdf.
[5] https://webdosya.csb.gov.tr/db/cbs/icerikler/2005-20180522115122.pdf.
[6] https://kamusm.bilgem.tubitak.gov.tr/dosyalar/mevzuat/kanunlar/kanun.pdf.
[7] www.resmigazete.gov.tr/eskiler/2004/10/20041012.htm#1.
[8] http://www.bilgitoplumu.gov.tr/Documents/1/BT_Strateji/Diger/060500_BilgiToplumuStratejisi.pdf.
[9] https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5651.pdf.
[10] https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5809.pdf.
[11] www.btk.gov.tr/siber-guvenlik-kurulu.
[12] https://bilgem.tubitak.gov.tr/en/sge/.

Investigación en Informática y Seguridad de la Información (BİLGEM) del Consejo de Investigación Científica y Tecnológica de Türkiye (TÜBİTAK) se estableció en el mismo año.

Estos hitos marcan un avance significativo en este ámbito. Como se ha mencionado anteriormente, en el marco del Sistema de Gobierno Parlamentario era en Türkiye, el Consejo de Ministros aprobó una decisión sobre la ejecución, gestión y coordinación de los Estudios Nacionales de Ciberseguridad el 11 de junio de 2012[13]. Con esta decisión se creó el Consejo de Ciberseguridad[14] y se encargó al Ministerio de Transportes, Asuntos Marítimos y Comunicaciones (ahora Ministerio de Transportes e Infraestructuras)[15], como se llamaba entonces, que desempeñara la secretaría del Consejo y coordinara las actividades de ciberseguridad con las instituciones pertinentes.

En la última década, se ha producido un notable aumento del ritmo de los avances en el sector de la ciberseguridad de Türkiye. Entre los principales hitos figuran el lanzamiento de la primera Estrategia Nacional de Ciberseguridad y Plan de Acción del país para 2013-2014[16], la creación del Centro Nacional de Respuesta a Incidentes Cibernéticos (USOM)[17] en el seno de la Autoridad de Tecnologías de la Información y las Comunicaciones (BTK)[18] y la publicación de una declaración en la que se esbozan la creación, las funciones y los principios de trabajo de los equipos de respuesta a incidentes cibernéticos[19]. Además, se crearon equipos de respuesta a incidentes cibernéticos (equipos institucionales de respuesta a incidentes cibernéticos, equipos sectoriales de respuesta a incidentes cibernéticos) en las instituciones y organizaciones públicas en el marco de la Estrategia Nacional de Ciberseguridad y Plan de Acción 2013-2014. Los equipos de respuesta a incidentes cibernéticos son organizaciones institucionales y sectoriales creadas para identificar rápidamente amenazas y ataques potenciales en el ciberentorno, y para desarrollar y compartir medidas para resolver los problemas causados por estos ataques. El objetivo de estos equipos es, por tanto, proporcionar competencias de ciberrespuesta a instituciones y organizaciones. En la actualidad, 14 equipos sectoriales de respuesta a incidentes cibernéticos operan bajo la coordinación del Centro Nacional de Respuesta a Incidentes Cibernéticos (USOM), y más de 2.100 equipos institucionales de respuesta a incidentes cibernéticos trabajan diligentemente para salvaguardar el ámbito cibernético de Türkiye.

El Centro de Ciberdefensa, creado en las Fuerzas Armadas turcas en 2012, ha evolucionado desde entonces hasta convertirse en el Mando de Ciberdefensa. Del mismo modo, el Departamento de Lucha contra los Ciberdelitos, que se instituyó en el seno de la Dirección General de Seguridad en 2011, se reestructuró posteriormente, en 2013.

La Ley núm. 6518[20], publicada en 2014, introdujo algunas normas en el ámbito de la ciberseguridad añadiendo artículos a la Ley núm. 5809, publicada en 2008, que regula el sector de las comunicaciones electrónicas. Con los artículos añadidos a la Ley núm. 5809, se creó el Consejo de Ciberseguridad, formado por altos cargos de instituciones públicas, bajo la presidencia del Ministerio de Transportes, Asuntos Marítimos y Comunicaciones. Con el apartado h) añadido al artículo 5 de la citada

[13] https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf.
[14] www.btk.gov.tr/siber-guvenlik-kurulu.
[15] www.uab.gov.tr/.
[16] https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/actionplan2013-2014.pdf.
[17] www.usom.gov.tr/.
[18] www.btk.gov.tr/.
[19] www.usom.gov.tr/hakkimizda.
[20] www.resmigazete.gov.tr/eskiler/2014/02/20140219-1.htm.

ley, se asignaron al Ministerio de Transporte, Asuntos Marítimos y Comunicaciones las funciones de "determinar políticas, estrategias y objetivos para garantizar la ciberseguridad nacional, preparar planes de acción y llevar a cabo actividades de educación y concienciación en materia de ciberseguridad".

Con este reglamento, el Consejo de Ciberseguridad ha sido designado como la principal autoridad responsable de la aprobación final y la aplicación efectiva de las políticas, estrategias y planes de acción en el país determinados por el Ministerio de Transporte, Asuntos Marítimos y Comunicaciones. El Consejo también se encarga de decidir sobre propuestas relacionadas con la identificación de infraestructuras críticas y de determinar las instituciones y organizaciones que deben quedar exentas de todas o parte de las disposiciones relacionadas con la ciberseguridad.

En 2016 se publicaron la Ley núm. 6698 de Protección de Datos Personales[21] y la Estrategia Nacional de Ciberseguridad y Plan de Acción[22] para 2016-2019. Además, con el Decreto Ley núm. 671[23], elaborado en consonancia con las necesidades del período, se autorizó a la Autoridad de Tecnologías de la Información y las Comunicaciones (BTK) con la declaración: "La Autoridad adoptará o exigirá que se adopten todo tipo de medidas para proteger a las instituciones y organizaciones públicas y a las personas físicas y jurídicas contra los ciberataques y para disuadir de estos ataques". Posteriormente, en 2017, bajo la coordinación de la Presidencia de Industrias de Defensa (ahora la Secretaría de Industrias de Defensa)[24], se inició la creación del Grupo Turco de Ciberseguridad, se completaron los nombramientos del Consejo de Protección de Datos Personales y este inició sus actividades.

En 2018, el Consejo de Ciberseguridad fue suprimido tras la publicación del Decreto Ley núm. 703[25]. Se declaró que las responsabilidades y el mandato del Consejo se transferirían a un "consejo o autoridad que designará el Presidente". Sin embargo, a pesar de algunos nombramientos parciales relacionados con estas responsabilidades, ninguno de ellos ha sido transferido oficialmente a ningún consejo o autoridad hasta la fecha. Con la transición al Sistema de Gobierno Presidencial, también se han producido cambios en el proceso de elaboración de políticas. La autoridad para formular políticas se ha transferido al Presidente de la República. Los Consejos de Política se han encargado de formular y desarrollar estas políticas (Decreto Presidencial núm. 1[26], arts. 20-22), mientras que los Ministerios son responsables de aplicarlas.

A partir del 10 de julio de 2018, con la implementación del Decreto Presidencial núm. 1 del Sistema Presidencial de Gobierno, la responsabilidad de "desarrollar propuestas de políticas y estrategias relacionadas con la ciberseguridad" se asignó al Consejo de Seguridad y Políticas Exteriores que opera bajo el Presidente (Decreto Presidencial núm. 1, artículo 36/1/ğ). Con el Decreto Presidencial núm. 1, la responsabilidad de "desarrollar proyectos para mejorar la seguridad de la información y la ciberseguridad" se asignó a la Oficina de Transformación Digital[27] de la Presidencia de la República de Türkiye, y en particular al Departamento de Ciberseguridad[28] dependiente de la Oficina de Transformación Digital. Entre las obligaciones del Departamento figuran las siguientes:

[21] https://kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law.
[22] https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/ulusalsibereng.pdf.
[23] www.resmigazete.gov.tr/eskiler/2016/08/20160817-18..htm.
[24] www.ssb.gov.tr/Default.aspx?LangID=2.
[25] https://www.resmigazete.gov.tr/eskiler/2018/07/20180709M3-1.pdf.
[26] https://www.mevzuat.gov.tr/mevzuatmetin/19.5.1.pdf.
[27] https://cbddo.gov.tr/en/.
[28] https://cbddo.gov.tr/en/department-of-cyber-security/.

- Desarrollar estrategias de ciberseguridad para instituciones públicas e infraestructuras críticas, en línea con las políticas establecidas por el Presidente.
- Seguimiento de los avances para aplicar eficazmente las políticas, estrategias y planes de acción nacionales en materia de ciberseguridad.
- Realizar investigaciones para identificar las infraestructuras críticas.
- Impulsar la cooperación entre los sectores público y privado y las universidades para fomentar un ecosistema nacional de ciberseguridad.
- Realizar estudios para desarrollar productos de ciberseguridad nacionales y domésticos en todos los sectores, especialmente en infraestructuras críticas, y promover su uso en el sector público.
- Realización de actividades preventivas y de protección para salvaguardar los activos críticos de tecnología e información.
- Realización de estudios sobre el establecimiento y la gestión del sistema de seguridad de la información en instituciones públicas y organizaciones que gestionan infraestructuras críticas; Esto incluye establecer normas y procedimientos técnicos, así como principios para supervisar y dirigir las aplicaciones.

Además, se creó la Dirección Nacional de Tecnología[29], dependiente del Ministerio de Industria y Tecnología[30], como se indica en el Decreto Presidencial núm. 1, publicado en la Gaceta Oficial de fecha 10 de julio de 2018. La Dirección recibió las siguientes responsabilidades en materia de ciberseguridad:

- Mejorar el nivel de madurez de la ciberseguridad y la seguridad de la información para la tecnología de la información y los productos y sistemas de tecnología avanzada.
- Desarrollo de productos nacionales y domésticos en ciberseguridad.
- Ampliar el uso de productos nacionales y nacionales en todo el país.
- Mejorar el centro de datos y la infraestructura de procesamiento de datos, y
- Apoyo al ecosistema de la ciberseguridad mediante diversos programas de incentivos.

En resumen, diversas leyes, reglamentos y otras legislaciones han designado varias instituciones para supervisar la ciberseguridad nacional. Estas instituciones derivan sus obligaciones relacionadas con la ciberseguridad de estas diferentes legislaciones. Al igual que en la mayoría de los demás países, la ciberseguridad en Türkiye se considera una responsabilidad compartida entre múltiples entidades gubernamentales. La Oficina de Transformación Digital y el Ministerio de Transportes e Infraestructuras han realizado estudios relacionados con el desarrollo de estrategias y políticas de ciberseguridad. Cada organización tiene su propio conjunto de funciones y responsabilidades dentro de su ámbito respectivo.

### 2. Funciones y responsabilidades de la Oficina de Transformación Digital en materia de ciberseguridad

Tras la transición al Sistema de Gobierno Presidencial en 2018, se creó la Oficina de Transformación Digital de la Presidencia de la República de Türkiye en virtud del Decreto Presidencial núm. 1, que entró en vigor tras su publicación en el Boletín Oficial de fecha 10 de julio de 2018. El mandato de la Oficina de

[29] www.sanayi.gov.tr/merkez-birimi/c03f1f3bae27/hakkimizda.
[30] www.sanayi.gov.tr/anasayfa.

Transformación Digital se amplió posteriormente mediante el Decreto Presidencial núm. 48 publicado el 24 de octubre de 2019[31].

La creación de la Oficina de Transformación Digital marcó una nueva era y un cambio de mentalidad respecto a los esfuerzos de digitalización en Türkiye. Desde su creación, se ha iniciado un enfoque interinstitucional más coherente y holístico de la transformación digital en el sector público. En consecuencia, además de lograr una administración más rápida, transparente y eficaz, su objetivo es coordinar, gestionar y operar de forma centralizada las actividades de transformación digital llevadas a cabo por separado en el marco de distintas instituciones, en consonancia con el desarrollo de las tecnologías, las demandas sociales y las tendencias de reforma del sector público. Además, su objetivo es coordinar las actividades relacionadas con la ciberseguridad, las tecnologías nacionales, los macrodatos y la inteligencia artificial (IA), tanto estratégicamente como en la práctica, bajo un mismo techo y aplicar eficazmente estrategias de alto nivel. Como resultado, bajo la coordinación de la Oficina de Transformación Digital, se establecen objetivos a nivel macro y se llevan a cabo iniciativas para proteger las infraestructuras digitales de Türkiye y para que se convierta en una ciberpotencia disuasoria.

La Oficina de Transformación Digital tiene las siguientes responsabilidades en el ámbito de la ciberseguridad: elaboración de políticas y normativas, creación de un ecosistema de ciberseguridad, concienciación pública, desarrollo de capacidades, refuerzo de las infraestructuras públicas y elaboración de normas:

- Desarrollar estrategias de ciberseguridad para las instituciones públicas y para las infraestructuras críticas de acuerdo con las políticas determinadas por el Presidente.
- Desarrollar proyectos de apoyo a la ciberseguridad nacional y la seguridad de la información.
- Seguimiento de la evolución de la aplicación efectiva a escala nacional de las políticas, estrategias y planes de acción en materia de ciberseguridad.
- Trabajar en la determinación de infraestructuras críticas.
- Hacer propuestas a los organismos relacionados sobre aquellas instituciones y organizaciones que queden exentas de la totalidad o parte de las disposiciones sobre ciberseguridad.
- Contribuir a la creación de un ecosistema nacional de ciberseguridad potenciando la colaboración entre el sector público, el privado y las universidades.
- Determinar áreas prioritarias de ciberseguridad para dirigir la capacidad del sector privado a campos críticos y evitar inversiones repetitivas.
- Trabajar en el desarrollo de productos de ciberseguridad locales y nacionales en todos los ámbitos, incluidas, principalmente, las infraestructuras críticas, y ampliar el uso de dichas soluciones en el sector público.
- Trabajar en actividades preventivas y de protección de activos críticos de tecnología e información.
- Establecer y poner en funcionamiento un sistema de gestión de la seguridad de la información en las instituciones públicas y en las organizaciones que explotan infraestructuras críticas, determinando normas y procedimientos técnicos y principios, y supervisando y orientando su aplicación.

[31] https://cbddo.gov.tr/en/governance-and-responsibilities.

En la actualidad, la Oficina de Transformación Digital es la máxima autoridad que gestiona los temas de ciberseguridad para las instituciones públicas y sectores críticos de nuestro país. Además de desempeñar las responsabilidades de la junta de ciberseguridad, colabora con todas las instituciones para coordinar el desarrollo y la ejecución eficaz de estrategias y planes de acción en todo el país.

### 3. Actividades y proyectos de la Oficina de Transformación Digital sobre elaboración de políticas

Aunque existen diferentes definiciones del concepto de ciberseguridad, una definición simple e inclusiva puede expresarse como una disciplina de seguridad aplicada a cada punto del ciberespacio que engloba los componentes de las tecnologías de la información. Dado que la Industria 4.0 se considera una revolución que pretende aunar las tecnologías de la información y todos los mecanismos vitales, es de esperar que la disciplina de la ciberseguridad se integre en nuestra disciplina vital como una adaptación de seguridad de esta revolución.

Cuando no se actúa conforme a la disciplina de seguridad, surgen problemas de seguridad y privacidad. Si se consideran a escala nacional, pasan a primer plano los objetivos estratégicos de proteger las infraestructuras críticas, garantizar el intercambio seguro de datos entre instituciones y organizaciones y mantener dentro del país el tráfico de datos cuyo origen y destino sea nacional. Su objetivo es aumentar el nivel de preparación frente a los ciberincidentes a escala institucional, sectorial y nacional mediante planteamientos basados en el análisis y la planificación en función de los riesgos.

Para garantizar la seguridad en el mundo digital, los gobiernos preparan y publican estrategias de ciberseguridad y garantizan su realización y supervisión asignando a las instituciones pertinentes. Nuestro país también cumple con su deber en este sentido. Como resultado del trabajo de nuestro país en esta materia bajo la coordinación del Ministerio de Transportes e Infraestructuras, a continuación se enumeran las estrategias publicadas respectivamente:

- Estrategia Nacional de Ciberseguridad y Plan de Acción 2013-2014[32]
- Estrategia Nacional de Ciberseguridad y Plan de Acción 2016-2019[33]
- Estrategia Nacional de Ciberseguridad y Plan de Acción 2020-2023[34]

La Estrategia Nacional de Ciberseguridad y los Planes de Acción mencionados avanzan con un enfoque holístico para garantizar la continuidad e incluyen medidas para garantizar la seguridad de las nuevas tecnologías que han entrado en nuestras vidas.

La última Estrategia Nacional de Ciberseguridad y Plan de Acción (2020-2023)[35] se publicó el 28 de diciembre de 2020 con el apoyo de la Oficina de Transformación Digital. Su objetivo es apoyar el desarrollo económico de nuestro país, proteger la vida social y la seguridad nacional y posicionar a nuestro país como marca internacional en el ámbito de la ciberseguridad. En este sentido, la Estrategia se centra en las políticas relacionadas con el período de cuatro años, en consonancia con la visión y la misión de ciberseguridad de Türkiye, y tiene como objetivo promover los logros alcanzados a través de estrategias

[32] https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/actionplan2013-2014.pdf.
[33] https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/ulusalsibereng.pdf.
[34] https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/national-cyber-security-strategy-2020-2023.pdf.
[35] https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/national-cyber-security-strategy-2020-2023.pdf.

anteriores. Los objetivos estratégicos determinados por la Estrategia Nacional de Ciberseguridad y Plan de Acción (2020-2023) se agruparon en ocho pilares:

- Proteger las infraestructuras críticas y aumentar la resiliencia
- Creación de capacidad nacional
- Red de ciberseguridad orgánica
- Seguridad de las tecnologías de nueva generación
- Lucha contra la ciberdelincuencia
- Desarrollo y fomento de las tecnologías nacionales
- Integración de la ciberseguridad en la seguridad nacional
- Mejora de la cooperación internacional

### 3.1 Sistema de seguimiento de la estrategia y el plan de acción

El Sistema de Seguimiento de la Estrategia y el Plan de Acción se ha desarrollado para gestionar y supervisar eficazmente la estrategia y los planes de acción preparados por la Presidencia, así como las actividades del Clúster Turco de Ciberseguridad dentro de la Oficina de Transformación Digital. El sistema sigue la evolución de las acciones y evalúa sus resultados y logros en función de objetivos predeterminados.

Además, la Oficina de Transformación Digital es responsable de apoyar las actividades de desarrollo de políticas coordinadas por el Consejo de Políticas de Ciencia, Tecnología e Innovación, entre las que se incluyen:

- Propuesta de Política Nacional de Ciberseguridad y Tecnologías de Infraestructuras de Comunicación
- Propuesta de política nacional para las tecnologías de comunicación de nueva generación 5G y posteriores
- Hoja de ruta nacional para las tecnologías de ciberseguridad

### 3.2 Medidas del Programa Presidencial Anual 2023

Sobre la base de la Estrategia Nacional de Ciberseguridad y Plan de Acción (2020-2023), las medidas del Programa Anual de la Presidencia 2023[36] de las que la Oficina de Transformación Digital es directamente responsable o con las que está relacionada son las siguientes:

- Se actualizará la Estrategia Nacional de Ciberseguridad, se reforzarán la normativa y la infraestructura técnica de ciberseguridad y se establecerá una sólida estructura de coordinación.
  - Se preparará una legislación marco sobre ciberseguridad.
  - Se prepararán la Estrategia Nacional de Ciberseguridad y el Plan de Acción 2024-2027.
- Se determinarán y pondrán en práctica procedimientos y principios para el establecimiento de sistemas de gestión de la seguridad de la información en infraestructuras críticas.

[36] https://www.sbb.gov.tr/wp-content/uploads/2022/11/2023-Yili-Cumhurbaskanligi-Yillik-Programi.pdf.

  - Se actualizará la Guía de Seguridad de la Información y las Comunicaciones.

- Con el fin de beneficiar al ecosistema de la ciberseguridad y desarrollar productos y soluciones con mayor valor añadido en este campo, se desarrollarán productos y proyectos tecnológicos de ciberseguridad en los que participen instituciones públicas de investigación y universidades, y los resultados de estos proyectos se compartirán con el ecosistema de la ciberseguridad en código fuente abierto.

- Se realizarán esfuerzos para reforzar el ecosistema nacional de ciberseguridad y aumentar su competitividad internacional.

  - Se organizará un foro empresarial internacional sobre ciberseguridad.

  - Se pondrá en marcha la Plataforma de Difusión de Productos Nacionales de Ciberseguridad para desarrollar un ecosistema que permita la maduración y exportación de los productos nacionales de ciberseguridad necesarios.

- Con el fin de formar una mano de obra cualificada en el ámbito de la ciberseguridad, se elaborarán planes de estudios de ciberseguridad para las escuelas de formación profesional y se establecerán normas profesionales.

  - Se mejorarán los actuales planes de estudios de ciberseguridad de las escuelas de formación profesional con planes de estudios de ciberseguridad.

  - Se determinarán los títulos profesionales de los estudiantes que se gradúen en centros de formación profesional con un plan de estudios en el campo de la ciberseguridad y se prepararán normas al respecto.

### 3.3. Medidas del Programa Presidencial Anual 2024

Sobre la base de la Estrategia Nacional de Ciberseguridad y Plan de Acción (2020-2023), las medidas del Programa Anual de la Presidencia 2024[37] de las que la Oficina de Transformación Digital es directamente responsable o con las que está relacionada son las siguientes:

- Se incrementará la ciberresiliencia y el nivel de madurez de la seguridad frente a las amenazas de ciberseguridad para los mercados financieros.

  - Se publicará un reglamento sobre la garantía de la ciberseguridad nacional y la mejora de la ciberdisuasión para cubrir el sector financiero.

- Se apoyará la armonización con las normas internacionales en el ámbito de la ciberseguridad y la participación de Türkiye en proyectos conjuntos internacionales.

  - Teniendo en cuenta las normas internacionales y la legislación de la Unión Europea, se ultimará la legislación derivada sobre la seguridad de la Internet de los objetos.

- Se promulgará una normativa para garantizar la ciberseguridad nacional teniendo en cuenta la Directiva de la Unión Europea sobre seguridad de las redes y de la información (NIS2) y sus nuevos esfuerzos en materia de ciberseguridad, así como las mejores prácticas internacionales.

[37] https://www.sbb.gov.tr/wp-content/uploads/2023/10/2024-Yili-Cumhurbaskanligi-Yillik-Programi.pdf.

  - Se publicará un reglamento para garantizar la ciberseguridad nacional y aumentar la ciberdisuasión.
  - Se llevarán a cabo estudios de regulación para la seguridad del Internet de las cosas.
  - Se llevarán a cabo inspecciones de ciberseguridad para los dispositivos del Internet de las cosas.
  - Se determinará la normativa secundaria necesaria en relación con la legislación marco nacional sobre ciberseguridad, cuyos trabajos preparatorios están en curso.
  - Se trabajará en la Ley de Firma Electrónica núm. 5070 y otras leyes pertinentes para proporcionar una base jurídica al servicio de firma a distancia.
  - Se llevarán a cabo actividades de sensibilización para ampliar el uso del servicio de firma a distancia en las instituciones públicas y el sector privado.

- Se garantizará la coordinación al más alto nivel de las actividades nacionales de ciberseguridad y se establecerá una estructura eficaz de coordinación y administración para fomentar la cooperación interinstitucional.
  - Se publicará una legislación exclusiva sobre ciberseguridad que regulará las funciones, obligaciones y responsabilidades de la organización nacional de ciberseguridad.
  - Se coordinarán los trabajos preparatorios de la Estrategia Nacional de Ciberseguridad y Plan de Acción 2024-2028 y se desarrollará un mecanismo de seguimiento de las actuaciones y actividades en el entorno digital.
  - Se llevarán a cabo esfuerzos para establecer un plan nacional de gestión de crisis y emergencias de ciberseguridad.
  - Se reforzará la red de intercambio de información sobre ciberamenazas
- Se reforzarán los procesos de adquisición e intercambio de información sobre ciberamenazas mediante el aumento de la diversidad de recursos y el desarrollo de aplicaciones de inteligencia artificial y análisis de macrodatos, y se llevarán a cabo esfuerzos para la detección temprana y la prevención de amenazas a la ciberseguridad nacional.
- Se llevará a cabo un análisis de las necesidades de recursos de inteligencia sobre ciberamenazas.
- Se aumentará la capacidad de respuesta y coordinación ante incidentes.
- Se iniciarán trabajos para proyectos de ciberseguridad apoyados en inteligencia artificial y análisis de big data para detectar dominios de phishing, centros de mando y control de malware y botnets.
- Se determinarán y pondrán en práctica procedimientos y principios para el establecimiento de sistemas de gestión de la seguridad de la información en infraestructuras críticas.
  - Se llevará a cabo un análisis de procesos para el establecimiento de un sistema de gestión de la seguridad de la información en infraestructuras críticas.

  - Se llevarán a cabo trabajos normativos para el establecimiento de un sistema de gestión de la seguridad de la información en infraestructuras críticas.

- Se establecerán normas de ciberseguridad en ámbitos de interés.
  - Se examinará el marco de certificación establecido en virtud de la Ley de Ciberseguridad de la Unión Europea y se determinarán las normas necesarias para los productos, servicios y procesos de ciberseguridad.
  - Los artículos relacionados con las directrices de seguridad de la información y las comunicaciones de la industria se incorporarán a la Guía de Seguridad de la Información y las Comunicaciones.
  - Se desarrollará un modelo para identificar las empresas críticas que deben someterse a auditoría en el marco de la Guía de Seguridad de la Información y las Comunicaciones.
  - Los preparativos para el proceso de auditoría se realizarán de conformidad con la Guía de Seguridad de la Información y las Comunicaciones.
  - Se llevarán a cabo actividades de sensibilización sobre la Guía de Seguridad de la Información y las Comunicaciones.
- Se desarrollarán infraestructuras de prueba para la ciberseguridad.
  - Se realizará un análisis de la situación actual de los centros de investigación y aplicación de la ciberseguridad, los bancos de pruebas de ciberseguridad y los laboratorios de integración de las universidades.
- Se incrementará el uso de productos nacionales de ciberseguridad, especialmente por parte de las instituciones públicas.
  - Se preparará una hoja de ruta para el desarrollo del sector de la ciberseguridad y su participación en el mercado mundial.
- Se desarrollarán programas para formar una mano de obra cualificada y mejorar las oportunidades profesionales en el campo de la ciberseguridad.
  - Se organizarán concursos de ciberseguridad para jóvenes empleados cualificados.
  - Se llevarán a cabo actividades de cooperación y coordinación para determinar las normas profesionales del personal que trabaja en el ámbito de la ciberseguridad.
- Se mejorarán los contenidos, la calidad y el entorno de la formación para capacitar a la mano de obra en consonancia con las necesidades del sector de la ciberseguridad.
  - Se impartirán cursos de ciberseguridad en línea y en laboratorio.
  - La formación en ciberseguridad en línea continuará a través de la Academia de la Autoridad de Tecnologías de la Información y las Comunicaciones (BTK).
  - Las formaciones en ciberseguridad aplicada se impartirán en el Centro de Formación Cibernética de la FETIH.
- Se realizarán estudios para concienciar a la población sobre la ciberseguridad.
  - Se llevarán a cabo estudios para desarrollar contenidos de cursos sobre ciberseguridad a nivel de educación primaria y secundaria.

  - Se desarrollará un proceso y programa de capacitación sobre concienciación en materia de seguridad de la información en relación con el cumplimiento y la auditoría de la Guía de Seguridad de la Información y las Comunicaciones.
  - Se organizarán actividades como seminarios, cursos de formación y concursos para concienciar sobre la ciberseguridad.
- Se reforzarán los mecanismos para la aplicación de medidas de seguridad de la información y las comunicaciones, el establecimiento, el funcionamiento y la auditoría de los sistemas de gestión de la seguridad de la información en las instituciones públicas.
  - Se establecerán normas secundarias para los procedimientos y principios que garanticen la seguridad de la información y las comunicaciones.
  - Se llevarán a cabo estudios de legislación e infraestructura sobre el uso y control de los nombres de dominio pertenecientes a instituciones y organizaciones públicas.

## 4. Actividades y proyectos de la Oficina de Transformación Digital sobre normativa y directrices de ciberseguridad

La Oficina de Transformación Digital ha llevado a cabo importantes actividades para aumentar la resiliencia nacional adoptando medidas para proteger tanto al sector público como al privado frente a las ciberamenazas. Entre los principales objetivos de estos esfuerzos figuran la mejora de las normativas y políticas de ciberseguridad, el establecimiento de mecanismos de auditoría, la prevención del bloqueo de proveedores en infraestructuras críticas, la garantía de una transformación tecnológica segura y la protección de los datos del país. A continuación se resumen algunos estudios en curso:

- Se ha elaborado un proyecto de reglamento para definir los procedimientos y principios relativos a la seguridad de los sitios web alojados por instituciones y organizaciones públicas y la asignación de subdominios “gov.tr”.
- Se ha elaborado un proyecto de reglamento para garantizar la seguridad de la información y las comunicaciones, con el fin de establecer requisitos técnicos para la aplicación de medidas de seguridad de la información y las comunicaciones. Además, el proyecto de reglamento incluye disposiciones para el establecimiento, la aplicación, el mantenimiento, la auditoría y la mejora continua de un sistema de gestión de la seguridad de la información para prevenir o mitigar los riesgos para la seguridad de la información. Los requisitos establecidos en este proyecto de reglamento están destinados a aplicarse a todas las instituciones públicas.
- Se está preparando una ley nacional de ciberseguridad. La Ley pretende abordar la gobernanza y la organización de la ciberseguridad nacional a través de un “Marco de Gobernanza de la Ciberseguridad” único, compatible con los avances tecnológicos y que aumentará la resiliencia nacional frente a las ciberamenazas actuales.

El resto de esta sección resume las iniciativas que se han aplicado o completado.

### 4.1 Circular presidencial sobre medidas de seguridad de la información 2019/12

La creciente digitalización de la información, la facilidad de acceso directo a la información, la digitalización de las infraestructuras y la proliferación de sistemas de

gestión de la información conllevan graves riesgos para la seguridad. En este contexto, se publicó la Circular Presidencial sobre Medidas de Seguridad de la Información 2019/12[38] para reducir los riesgos de seguridad encontrados y garantizar la seguridad de los tipos de datos críticos que pueden amenazar la seguridad nacional o alterar el orden público. La Circular incluye 21 medidas básicas de seguridad de la información y las comunicaciones[39] que deben seguir las instituciones públicas y el sector privado que ofrecen servicios de infraestructuras críticas. Para garantizar la protección de datos, la Circular Presidencial pretende asegurar que los datos propiedad de un país permanezcan dentro de las fronteras de ese país. Además, destaca que la producción y el uso de soluciones nacionales de ciberseguridad representan una de las principales prioridades de Türkiye. Por último, también establece que "se elaborará una Guía de Seguridad de la Información y las Comunicaciones bajo la coordinación de la Oficina de Transformación Digital con el fin de mitigar y neutralizar los riesgos de seguridad y especialmente garantizar la seguridad de los datos críticos".

### 4.2 Guía de Seguridad de la Información y las Comunicaciones

A raíz de la Circular Presidencial sobre Medidas de Seguridad de la Información 2019/12 mencionada anteriormente, en 2020 se publicó el documento Guía de Seguridad de la Información y las Comunicaciones[40]. El objetivo principal de la guía es determinar medidas detalladas de ciberseguridad para garantizar la seguridad de la información/datos e infraestructuras críticas que puedan provocar alteraciones del orden público o amenazar la seguridad nacional. La Guía es el primer documento nacional de referencia publicado en este ámbito y hace hincapié en la necesidad de una estrategia de seguridad global que abarque todos los aspectos de la seguridad de la información y las comunicaciones. Desempeña un papel importante en el fortalecimiento de las capacidades de ciberdefensa de las instituciones públicas y de los proveedores de servicios de infraestructura crítica. Además, tanto la Circular Presidencial sobre Medidas de Seguridad de la Información 2019/12 como la Guía de Seguridad de la Información y las Comunicaciones exigen a los vendedores de productos una declaración de que sus productos están libres de puertas traseras.

### 4.3 Guía de Auditoría de la Seguridad de la Información y las Comunicaciones

Con el fin de alcanzar y garantizar la continuidad de los logros previstos en la Guía de Seguridad de la Información y las Comunicaciones, la Oficina de Transformación Digital elaboró la Guía de Auditoría de la Seguridad de la Información y las Comunicaciones[41], que se publicó en octubre de 2021, reconociendo que la seguridad de la información y las comunicaciones es posible mediante actividades eficaces de auditoría y vigilancia.

Se espera que las instituciones públicas y las organizaciones y empresas que prestan servicios de infraestructuras críticas completen sus actividades de cumplimiento en el plazo especificado en la Guía de Seguridad de la Información y las Comunicaciones, y que lleven a cabo estudios de auditoría al menos una vez al año para garantizar el cumplimiento de las actividades realizadas y las medidas adoptadas.

Las organizaciones incluidas en el ámbito de aplicación no solo están obligadas a cumplir los requisitos de la Guía de Seguridad de la Información y las Comunicaciones, sino también a realizar auditorías y evaluaciones periódicas de la

[38] https://www.mevzuat.gov.tr/MevzuatMetin/CumhurbaskanligiGenelgeleri/20190706-12.pdf.
[39] cbddo.gov.tr/en/presidential-circular-no-2019-12-on-information-security-measures.
[40] cbddo.gov.tr/en/icsaguide/.
[41] cbddo.gov.tr/en/icsaguide/.

eficacia con que se aplican las medidas de seguridad y de si el proceso de aplicación se ajusta a los requisitos correspondientes. Por lo tanto, las auditorías periódicas, al menos una vez al año, deben ser llevadas a cabo por una función de auditoría interna o por terceras empresas de auditoría acreditadas. Las políticas y procedimientos de auditoría que deben llevar a cabo las organizaciones en cuestión están documentadas en la Guía de Auditoría de la Seguridad de la Información y las Comunicaciones, publicada por la Oficina de Transformación Digital en 2021.

### 4.4 Auditor de seguridad de la información y las comunicaciones/Programa de certificación de empresas

El Programa de Certificación de Empresas/Auditores de Seguridad de la Información y las Comunicaciones ha sido diseñado para proporcionar los conocimientos necesarios para determinar las cualificaciones y competencias de las empresas y auditores que llevarán a cabo las auditorías de conformidad con la Guía de Seguridad de la Información y las Comunicaciones. El Programa se lleva a cabo en cooperación con la Institución Turca de Normalización y el Consejo de Investigación Científica y Tecnológica de Türkiye (TÜBİTAK). Un total de 163 auditores y 23 empresas han sido certificados y autorizados en el marco del Programa de Certificación desde 2021.

### 4.5 Sistema de Control de Auditoría y Cumplimiento de la Seguridad de la Información y las Comunicaciones

El Sistema de Vigilancia del Cumplimiento y Auditoría de la Seguridad de la Información y las Comunicaciones[42] fue desarrollado y puesto en servicio el 4 de enero de 2023. El sistema permite supervisar los resultados de las auditorías de todas las organizaciones cubiertas por la Guía de Seguridad de la Información y las Comunicaciones. Desde entonces, ya se han registrado en el sistema 2.945 usuarios y 1.191 organizaciones. Las organizaciones pueden proporcionar información sobre el progreso de sus actividades de cumplimiento y auditoría de la Guía de seguridad de la información y las comunicaciones. El nivel actual de cumplimiento de los sistemas de gestión de la seguridad de la información de las organizaciones también puede rastrearse a través de esta plataforma digital.

### 4.6 Proyecto de análisis y elaboración de informes sobre el modelo nacional de gobernanza de la ciberseguridad

El Proyecto de Análisis e Información del Modelo Nacional de Gobernanza de la Ciberseguridad, que se inició para examinar el modelo de gobernanza de la ciberseguridad en Türkiye, ha finalizado. Se realizó un análisis comparativo revisando los casos de distintos países y se presentaron recomendaciones para la mejora. Como resultado, se desarrolló para Türkiye el “Marco de Gobernanza de la Ciberseguridad”.

Tras la finalización del proyecto, el 13 de diciembre de 2022 se organizó un Taller Nacional de Ciberseguridad para compartir los resultados del Proyecto de Análisis e Información del Modelo Nacional de Gobernanza de la Ciberseguridad. Más de 40 instituciones públicas y más de 100 participantes compartieron sus opiniones y sugerencias durante el taller. Según los resultados del taller, se determinó que es necesaria una ley nacional de ciberseguridad. Se está trabajando para ultimar esta ley.

[42] cbddo.gov.tr/en/bigdes/.

## 5. Actividades y proyectos de la Oficina de Transformación Digital sobre el ecosistema de la ciberseguridad

### 5.1 Clúster turco de ciberseguridad

En octubre de 2017, se invitó a las instituciones del sector público, al mundo académico y a las principales empresas de ciberseguridad del sector privado a debatir sobre la posible cooperación entre estos organismos, lo que dio lugar a la creación del Grupo Turco de Ciberseguridad[43]. En la actualidad, el clúster funciona bajo la coordinación de la Oficina de Transformación Digital y la Secretaría de Industrias de Defensa (SSB) con más de 200 miembros, que cuentan con más de 400 productos y servicios. Turkish Cyber Security Cluster también es miembro de Global Ecosystems Partnered in Innovation and Cybersecurity (Global EPIC) desde 2018.

El Cluster Turco de Ciberseguridad persigue varios objetivos, entre ellos:

- Aumento del número de empresas de ciberseguridad
- Apoyar el desarrollo de las capacidades técnicas, administrativas y financieras de las empresas miembros
- Mejorar la imagen de marca de los productos y servicios
- Mejorar las normas del ecosistema de ciberseguridad
- Aumentar la competitividad de las empresas miembros en los mercados nacional y mundial
- Mejorar el capital humano en el ámbito de la ciberseguridad
- Aumentar la concienciación sobre ciberseguridad en toda la sociedad

Aunque no existe obligación legal de que el sector privado participe en dicha cooperación, se mantiene el énfasis en la confianza mutua y la colaboración entre el sector público y las instituciones privadas. La principal motivación de este esfuerzo es reforzar las relaciones entre compradores y proveedores, los canales de distribución comunes, las oportunidades de establecer redes conjuntas y las actividades de investigación y desarrollo que llevan a cabo las universidades con las empresas y que pueden crear mejores oportunidades y beneficios para ambas partes. Debido a los intereses económicos compartidos, las empresas de la agrupación se volvieron más productivas, más innovadoras y, por tanto, más competitivas que las empresas que operaban solas.

Por lo general, no es posible alcanzar el éxito en el ámbito de la ciberseguridad sin el apoyo de la autoridad pública de más alto nivel. Türkiye tiene empresas que se han expandido al extranjero y productos de ciberseguridad cualificados y únicos que comercian en el extranjero. Algunos de estos productos también figuran en informes de Gartner. La categoría de simulación de violaciones y ataques es una de ellas.

### 5.2 Consejo de Relaciones Económicas Exteriores (DEİK) - Consejo Empresarial de Tecnologías Digitales (DIGITECH) - Comité de Ciberseguridad

Con el fin de aumentar la eficacia de nuestras empresas nacionales y nacionales en el extranjero, en junio de 2022 se puso en marcha el Consejo Empresarial de Tecnologías Digitales (DIGITECH)[44] con el apoyo de la Oficina de Transformación Digital y bajo la coordinación de la Junta de Relaciones Económicas Exteriores (DEİK). El Consejo Empresarial de Tecnologías Digitales (DIGITECH) se compromete a llevar a cabo proyectos sobre:

[43] https://siberkume.org.tr/.

[44] www.deik.org.tr/sectoral-business-councils-digital-technologies-business-council?pm=65.

- Globalización del ecosistema de tecnologías digitales de Türkiye
- Adaptarse a las nuevas tendencias
- Acceso a la financiación internacional, transformación digital y normativa

El objetivo de DIGITECH:

- Aumento del número de empresas turcas en Fortune 500 y del número de "unicornios" turcos (Turcons)
- Hacer de Türkiye un centro tecnológico y crear corredores digitales con otros países
- Potenciar la exportación de productos de alta tecnología de Türkiye
- Fomento de la internacionalización de las empresas tecnológicas a través de 144 consejos empresariales bilaterales de DEİK
- Apoyar la transformación digital de las empresas industriales asociándose con start-ups
- Aumentar el capital riesgo en el sector, tanto en tamaño como en número, mediante la creación de plataformas que reúnan a los capitales riesgo mundiales, los capitales riesgo nacionales, las *scale-ups* y las empresas emergentes
- Identificar los problemas a los que se enfrenta el sector e informar a los organismos gubernamentales respectivos sobre dichos problemas

Los subcomités de DIGITECH son los siguientes: Tecnología en la nube, Tecnologías financieras (Fintech), Tecnologías móviles, Juego, Ciberseguridad, Tecnologías de software, Tecnologías innovadoras, Capital riesgo, Tecnologías sanitarias, Web3-Blockchain. Como puede verse, en esta estructura, en la que la Ciberseguridad también es un subcomité, existe una perspectiva sectorial.

El desarrollo de tecnologías nacionales en el campo de la ciberseguridad es de importancia estratégica en Türkiye y se reconoce como una cuestión de seguridad nacional. Así, se hace hincapié en la creación de productos y servicios sólidos y a gran escala que puedan rivalizar con sus homólogos extranjeros. El mercado mundial de la ciberseguridad, impulsado por la creciente concienciación sobre los riesgos y amenazas para los datos, ha registrado recientemente un crecimiento significativo. Se prevé que la cuota de mercado de los productos y servicios de ciberseguridad siga aumentando.

Türkiye forma parte de esta economía en expansión, colaborando con el sector privado y las instituciones gubernamentales para desarrollar sus soluciones a escala mundial. En consecuencia, la Oficina de Transformación Digital está trabajando para reforzar las tecnologías nacionales de ciberseguridad. Este esfuerzo forma parte del mandato otorgado por el Decreto Presidencial núm. 1, que establece; Realizar estudios para desarrollar productos de ciberseguridad domésticos y nacionales en todos los ámbitos, especialmente en infraestructuras críticas, y extender su uso en el sector público.

Para fomentar el crecimiento del ecosistema nacional en ciberseguridad, se ha iniciado un enfoque sistemático bajo la coordinación de la Oficina de Transformación Digital. Este planteamiento pretende integrar el sistema de incentivos con la contratación pública, evaluar los niveles de madurez de los productos nacionales de ciberseguridad y mejorarlos y ampliarlos gradualmente.

El "Grupo de Coordinación Cibernética Nacional" se formó en 2021 bajo la coordinación de la Oficina de Transformación Digital, con el liderazgo de la Secretaría de Industrias de Defensa (SSB), el Ministerio de Industria y Tecnología

(MoIT), la Oficina de Suministros del Estado, la Agencia de Contratación Pública (KİK) y la Presidencia de Estrategia y Presupuesto (SBB). El Ministerio de Hacienda y Finanzas (MoTF), el Consejo de Investigación Científica y Tecnológica de Türkiye (TÜBİTAK), la Institución Turca de Normalización, TURKSAT, el Ministerio de Transportes e Infraestructuras y la Autoridad de Tecnologías de la Información y las Comunicaciones (BTK) se unieron posteriormente a este grupo. El objetivo principal es fomentar el uso de productos de ciberseguridad nacionales en todos los sectores, tanto a escala nacional como internacional, con especial atención al sector público. Las actividades del grupo se dividen en cinco pilares principales: política, legislación, normalización/madurez, incentivos/apoyo/financiación e internacionalización.

## 6. Actividades y proyectos de la Oficina de Transformación Digital sobre concienciación en materia de ciberseguridad

### 6.1 Concursos de ciberseguridad TeknoFest

La Oficina de Transformación Digital es consciente de que la necesidad de concienciación y competencias en materia de ciberseguridad es cada vez más urgente, dada la importancia que se atribuye a las tecnologías de la información y las comunicaciones (TIC). En este sentido, la Oficina de Transformación Digital también organiza concursos para aumentar la concienciación sobre ciberseguridad. Uno de los proyectos destacados es HackIstanbul. Está reconocido en todo el mundo como un concurso extraordinario y se celebra como parte del Festival de Aviación, Espacio y Tecnología TeknoFest[45] desde 2018. Estos concursos abrieron sus puertas a todos los hackers del mundo para mostrar su talento en Estambul, los concursos se celebraron bajo el nombre de “HackIstanbul”, y solo en 2020 el concurso se celebró en Gaziantep bajo el nombre: “HackZeugma”. En 2022, la Oficina de Transformación Digital organizó HackBlackSea 2022 en Zonguldak en agosto.

Las solicitudes para el concurso HackMasters 2023, que se celebró el 23 de abril de este año, se cerraron en marzo de 2023. Los finalistas se determinaron durante la fase de caza de recompensas en línea. En la fase final, celebrada el 28 de abril, se planteó a los concursantes un escenario centrado en la ciberseguridad de los dispositivos inteligentes. Los piratas informáticos intentaron comprometer los sistemas buscando vulnerabilidades en los dispositivos domésticos inteligentes, las aplicaciones móviles que los gestionan y las infraestructuras en la nube que reciben datos de estos dispositivos, tratando de apoderarse de los sistemas.

Cada año se abordan en los contenidos del concurso conceptos diferentes, como la seguridad de los sistemas tecnológicos operativos, la recompensa por fallos o el reto de ciberseguridad “capturar la bandera”. Estos concursos pretenden concienciar sobre la ciberseguridad y atraer nuevos talentos al sector. Por otro lado, un beneficio indirecto del proyecto es la promoción mundial de Türkiye en materia de ciberseguridad.

El plazo de presentación de candidaturas para HackMasters 2024[46] finaliza el 31 de mayo de 2024, y la fase final se celebrará en agosto de 2024 en Estambul, en el marco del TeknoFest[47].

### 6.2 Concurso de ciberinteligencia

Además, la Oficina de Transformación Digital organiza varios campamentos de ciberseguridad y programas de formación, así como eventos de “captura la bandera” con instituciones públicas pertinentes, como el Ministerio de Educación Nacional y

[45] www.teknofest.org/en/.
[46] https://hackmasters.com.tr/.
[47] www.teknofest.org/en/competitions/hack-masters/.

el Ministerio de Juventud y Deportes, el sector privado y organizaciones no gubernamentales. Estos campamentos y programas de formación garantizan que un número suficiente de jóvenes se sientan inspirados para utilizar su talento en ciberseguridad. También es importante señalar que el número de estudiantes que participan en estos acontecimientos supera el millón.

Además, el otro evento destacado es el Concurso de Ciberinteligencia[48]. Estos concursos forman parte de actividades de formación y concienciación cuyo objetivo es aumentar el número de personas concienciadas en ciberseguridad, y son muy eficaces en este sentido. Un total de 1,5 millones de estudiantes de primaria, secundaria y bachillerato participaron en el concurso.

El concurso es un evento en línea y se organiza por separado para los niveles de primaria, secundaria y bachillerato. Las preguntas son preparadas por la Oficina de Transformación Digital y finalizadas con el apoyo del Ministerio de Educación Nacional teniendo en cuenta el plan de estudios actual. Los anuncios se realizan a través de las cuentas de redes sociales de la Oficina de Transformación Digital, el Ministerio de Educación Nacional y la plataforma EBA (red de información educativa). En el concurso, los alumnos que den el mayor número de respuestas correctas en el menor tiempo posible reciben regalos sorpresa y recompensas para aumentar su motivación en este campo.

El cuarto Concurso de Conocimientos de Ciberinteligencia tuvo lugar en 2023. Este concurso, que se organizó por primera vez en octubre de 2020 en colaboración con la Presidencia y el Ministerio de Educación Nacional, está dirigido a los niveles de primaria, secundaria y bachillerato. El concurso se celebró el 27 de diciembre de 2023, para alumnos de primaria, el 28 de diciembre de 2023, para alumnos de secundaria, y el 29 de diciembre de 2023, para alumnos de bachillerato. El concurso contó con un total de 16.915 inscripciones de estudiantes de primaria, 15.955 de secundaria y 4.528 de bachillerato.

### 6.3 Dibujos animados de Digital Crew

Having conducted many studies on raising cybersecurity awareness on a national scale, the Digital Transformation Office also recognizes the need to increase digital literacy even when children are not online. Esto va más allá de los conocimientos técnicos. Se refiere a los conocimientos, habilidades y actitudes que permiten a los niños estar seguros y capacitados en un mundo digital. Uno de los proyectos importantes desarrollados con este fin dirigido a los niños es una popular serie de películas de dibujos animados llamada *Digital Crew*[49]. Se emite en la Radio y Televisión Turca Çocuk (“Kid”) desde 2020. El principal objetivo de este proyecto es aumentar el conocimiento, la alfabetización y la concienciación digitales de los niños. El contenido de la serie de *Digital Crew*, que consta de 10 episodios, se preparó en colaboración con la Oficina de Transformación Digital. Los episodios cubren una amplia gama de temas, desde la seguridad de los niños en Internet al ciberacoso, desde la adicción a Internet a la inteligencia artificial (IA), desde la Internet de las cosas al impacto de la digitalización en la vida y las tecnologías nacionales.

## 7. Actividades y proyectos de la Oficina de Transformación Digital sobre educación en ciberseguridad

Sin duda, uno de los componentes más importantes para garantizar la ciberseguridad nacional son unos recursos humanos con suficiente competencia y

[48] https://cbddo.gov.tr/en/projects/cyberintelligencecontest/.

[49] www.youtube.com/watch?v=YnuLs6GAogM&ab_channel=CBDijitalD%C3%B6n%C3%BC%C5%9F%C3%BCmOfisi.

experiencia. Con el fin de satisfacer las necesidades de nuestro país en este ámbito, la Oficina de Transformación Digital lleva a cabo actividades para aumentar el nivel de competencia de los recursos humanos existentes. A continuación se presentan algunas de ellas.

### 7.1 Escuela Superior Profesional de Ciberseguridad en cooperación con el Ministerio de Educación Nacional de la República de Türkiye

Se tomaron medidas concretas para desarrollar competencias y capacidades en el ámbito de la ciberseguridad en la educación formal y, como resultado, el plan de estudios desarrollado para el nivel de educación secundaria comenzó en 2020.

Teknopark Istanbul Vocational and Technical Anatolian High School, el primer instituto de ciberseguridad de Türkiye, fue creado por el Ministerio de Educación Nacional con la contribución del Clúster Turco de Ciberseguridad, la Secretaría de Industrias de Defensa (SSB), la Oficina de Transformación Digital y Technopark Istanbul. Situada en Teknopark Estambul, la escuela imparte enseñanza en los campos de tecnologías de la información, gestión de redes y ciberseguridad.

La Escuela Secundaria Profesional de Ciberseguridad ha estado en lo más alto de la lista de preferencias desde el día de su apertura.

### 7.2 Creación de escuelas profesionales de ciberseguridad en cooperación con el Consejo de Educación Superior de la República de Türkiye

La Oficina de Transformación Digital ha puesto en marcha un nuevo proyecto para formar personal cualificado en el ámbito de la ciberseguridad profundizando en el modelo aplicado en el Bachillerato Profesional de Ciberseguridad mencionado anteriormente. Con el protocolo de colaboración firmado entre la Oficina de Transformación Digital y el Consejo de Educación Superior[50] en 2022, se dio el primer paso para los Colegios Profesionales de Ciberseguridad.

Los centros de formación profesional en ciberseguridad, que ofrecerán programas educativos únicamente en el ámbito de la ciberseguridad, se inauguraron en 2023. El primer programa que se ofrece en estas escuelas es “Analista y Operador de Ciberseguridad”[51]. Este programa se ha puesto en marcha en cuatro de las principales universidades de Türkiye: la Universidad de Ankara, la Universidad Ege, la Universidad Técnica de Gebze y la Universidad Técnica de Estambul.

## 8. Türkiye en los índices mundiales

Como resultado de la adopción de tecnologías digitales a nivel local y nacional, la ciberseguridad se ha vuelto tan importante como la seguridad física para el país. Dada la creciente amenaza, se han realizado suficientes inversiones en el campo de la ciberseguridad en los sectores público y privado. Se han llevado a cabo numerosos proyectos coordinados en los ámbitos público, privado y militar; importantes organizaciones de la industria de defensa han realizado importantes inversiones; En el ámbito académico se han creado institutos específicos de ciberseguridad; y se han desarrollado nuevos productos y tecnologías con capacidades nacionales. Como resultado de estos esfuerzos, Türkiye se ha convertido recientemente en uno de los países con más éxito en el campo de la ciberseguridad.

Gracias a los esfuerzos del Gobierno y de los agentes del sector público por alcanzar estos objetivos, la clasificación de Türkiye en los índices mundiales de ciberseguridad se ha visto afectada positivamente. Türkiye disfruta de una alta

[50] https://cbddo.gov.tr/projeler/siber-myo/.
[51] cbddo.gov.tr/sss/siber-myo/.

clasificación en el Índice Global de Ciberseguridad, lo que refleja los logros del país hasta la fecha.

Según el Índice Mundial de Ciberseguridad publicado por la Unión Internacional de Telecomunicaciones (UIT) en 2021[52], Türkiye ocupa el undécimo lugar en el mundo, subiendo nueve puestos con respecto al año anterior, y el sexto en Europa.

En el panorama mundial actual, las TIC han asumido un papel indispensable. Son el sostén de nuestras sociedades, vinculando estrechamente economías, gobiernos e individuos a lo largo y ancho del planeta. Imaginar un mundo sin comunicación instantánea, acceso sin fisuras a la información o la posibilidad de hacer negocios por vía electrónica es imaginar una realidad fundamentalmente distinta. Las TIC han tenido un impacto demostrable en todas las facetas de la experiencia humana, desde la difusión del conocimiento y la prestación de asistencia sanitaria hasta los ámbitos del entretenimiento y la interacción social. Está empoderando a los ciudadanos, fomentando una innovación revolucionaria e impulsando el crecimiento económico a un ritmo sin precedentes. Además, los gobiernos pueden aprovechar el poder de las TIC para prestar servicios con mayor eficiencia, transparencia e inclusión, fomentando un marco democrático más participativo y sólido.

Sin embargo, aunque este paradigma de conectividad ofrece inmensas ventajas, también conlleva una importante advertencia: la seguridad. A medida que nuestra dependencia de las TIC aumenta sin cesar, también lo hace la vulnerabilidad a la que nos exponemos. Los actores maliciosos, que van desde ciberdelincuentes que buscan beneficios personales hasta entidades patrocinadas por el Estado con agendas geopolíticas, explotan estas vulnerabilidades para atacar infraestructuras críticas, sistemas gubernamentales que albergan datos sensibles e información personal de los ciudadanos. La naturaleza globalmente interconectada de la infraestructura de las TIC crea una compleja red de interdependencias, en la que un solo fallo de seguridad en un rincón remoto del mundo puede tener efectos en cascada en otros lugares, interrumpiendo potencialmente servicios esenciales, causando dificultades económicas y socavando la confianza pública. La aparición de nuevas tecnologías, como la inteligencia artificial y la Internet de las cosas, introduce toda una nueva dimensión de retos de seguridad que requieren atención inmediata y el desarrollo de soluciones innovadoras, ya que estas tecnologías suelen introducir nuevos vectores de ataque y complejidades a la hora de proteger vastas redes de dispositivos interconectados.

Por lo tanto, es imperativo recorrer cuidadosamente un camino que promueva un equilibrio sensato entre el aprovechamiento del inmenso potencial de las TIC y la mitigación de los riesgos asociados. Los Estados deben dar prioridad a la seguridad de las tecnologías de la información y las comunicaciones y reconocerla como un imperativo de seguridad nacional. Esto requiere un enfoque polifacético. El desarrollo de sólidas estrategias nacionales de ciberseguridad, apoyadas por fuertes asociaciones público-privadas que aprovechen la experiencia y los recursos tanto del gobierno como de la industria, es primordial.

Los esfuerzos de colaboración entre gobiernos y empresas para invertir en educación y concienciación en materia de ciberseguridad, tanto para los ciudadanos como para los funcionarios públicos, son igualmente críticos. Esta educación no solo debe incluir conocimientos técnicos para identificar y mitigar las ciberamenazas, sino también promover una cultura de ciberhigiene entre los ciudadanos.

[52] www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

Además, el fomento de la cooperación internacional en materia de seguridad de las TIC es innegablemente esencial. En este contexto, es muy importante mantener un diálogo institucional regular en el marco de las Naciones Unidas. Los Estados miembros deben colaborar para establecer un marco de normas, estándares y marcos jurídicos internacionales que promuevan un comportamiento responsable en el ciberespacio. Este marco debería incluir protocolos de intercambio de información para facilitar una respuesta rápida a las ciberamenazas, esfuerzos de cooperación policial para combatir más eficazmente la ciberdelincuencia y el desarrollo de tratados internacionales que establezcan normas de comportamiento aceptable en el ciberespacio. En última instancia, el objetivo va más allá de las medidas puramente defensivas, para construir una infraestructura de TIC resiliente. Ello incluye diseñar sistemas que no solo tengan la resistencia necesaria para soportar ciberataques, sino también la capacidad de recuperarse rápidamente, minimizar las interrupciones y mantener la integridad de los datos. Además, es importante promover el desarrollo y uso éticos de las TIC. Los Estados miembros pueden garantizar que esta poderosa tecnología sirva al bien mayor de los valores humanos dando prioridad a la privacidad de los usuarios, abogando por prácticas de investigación responsables que minimicen el potencial de uso indebido y garantizando la transparencia en el desarrollo y despliegue de los sistemas de TIC.

Al dar prioridad a la seguridad y fomentar al mismo tiempo la innovación, los Estados miembros pueden garantizar que las TIC sigan desempeñando un papel transformador y positivo en la configuración de nuestro mundo. Este enfoque colaborativo, unido a una vigilancia y adaptación continuas, es esencial para garantizar un futuro digital seguro y próspero para todos.

## Venezuela (República Bolivariana de)

[Original: español
26 de abril de 2024]

La resolución 78/237 de la Asamblea General, adoptada el 22 de diciembre de 2023, en su párrafo 8, invita a todos los Estados Miembros a que sigan informando al Secretario General de sus opiniones y observaciones sobre la seguridad de la tecnología de la información y las comunicaciones y de su uso, en particular sobre el futuro diálogo periódico sobre esas cuestiones que se celebrará bajo los auspicios de las Naciones Unidas, y solicita al Secretario General que en su septuagésimo octavo período de sesiones le presente un informe en el que se recojan dichas opiniones para que los Estados Miembros continúen deliberando en las reuniones del octavo período de sesiones del grupo de trabajo de composición abierta, en 2024.

En este sentido, la República Bolivariana de Venezuela considera que es menester recalcar la importancia del grupo de trabajo de composición abierta y su formato de trabajo, para cumplir el mandato de la Asamblea General, articulados en la resolución 75/240 de la Asamblea. Los logros en los últimos años —como la creación del directorio mundial intergubernamental de puntos de contacto— demuestran que el formato actual del grupo de trabajo de composición abierta ha sido bastante exitoso, particularmente a raíz de su dependencia en el consenso para la toma de decisiones y en la aprobación de los informes anuales.

La República Bolivariana de Venezuela considera que las Naciones Unidas deben seguir desempeñando un papel fundamental y central en la promoción del diálogo sobre el uso que hacen los Estados de la tecnología de la información y las comunicaciones. El carácter sui generis de la tecnología de la información y las comunicaciones, implica la necesidad de desarrollar nuevos principios y normas —preferiblemente jurídicamente

vinculantes— que permiten llenar los espacios que existen entre el derecho internacional existente y las realidades de un ámbito virtual.

En virtud de lo antes indicado, se considera como una urgente necesidad, el otorgamiento de una continuidad a las labores del grupo de trabajo de composición abierta del 2021 al 2025, a través de un nuevo grupo de trabajo de composición abierta permanente, a ser establecido después del 2025, lo cual ayudará a fortalecer la capacidad de esta nueva reiteración del grupo de trabajo de composición abierta para elaborar y adaptar nuevas normas jurídicamente vinculantes, y que ayuden a fortalecer la seguridad internacional en el uso de las tecnologías de las comunicaciones y la información.

Igualmente, es urgente dotar al próximo grupo de trabajo de composición abierta después del 2025 con la capacidad de abordar los desafíos que surgen de la gran brecha digital que existe entre los países miembros, brecha que hace difícil concretar estrategias globales para el fortalecimiento de la seguridad internacional en el uso de las tecnologías de las comunicaciones y la información.

Finalmente, se respaldan ampliamente los grandes esfuerzos del presidente del grupo de trabajo de composición abierta para lograr el consenso en todas las actividades de este grupo y se reitera la disposición de la República Bolivariana de Venezuela de continuar participando y apoyando en este proceso.

## Respuestas recibidas de organizaciones intergubernamentales

## Unión Europea

[Original: inglés
29 de abril de 2024]

El ciberespacio, y en particular la Internet mundial y abierta, se ha convertido en uno de los ejes principales de nuestras sociedades. Ofrece una plataforma que impulsa la conectividad y el crecimiento económico. La Unión Europea y sus Estados miembros apoyan un ciberespacio mundial, abierto, estable y seguro, sobre la base del estado de derecho, los derechos humanos, las libertades fundamentales y los valores democráticos que aportan el desarrollo social, económico y político a nivel mundial.

La comunidad internacional reconoce que el derecho internacional vigente —incluida la totalidad de la Carta de las Naciones Unidas— es aplicable a la conducta de los Estados en el ciberespacio y es esencial para mantener la paz y la estabilidad y promover un entorno abierto, seguro, pacífico y accesible para las TIC.

Las recomendaciones por consenso formuladas en 2010, 2013, 2015 y 2021 por el Grupo de Expertos Gubernamentales sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, la recomendación por consenso de 2021 del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Comunicaciones en el Contexto de la Seguridad Internacional y los informes anuales de 2022 y 2023 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) han desarrollado y consolidado un marco de comportamiento responsable de los Estados en el ciberespacio. Este marco comprende la aplicación del derecho internacional al ciberespacio, normas voluntarias de comportamiento responsable de los Estados, medidas de fomento de la confianza y creación de capacidad.

La Unión Europea y sus Estados miembros reafirman su determinación de actuar de conformidad con estos acuerdos vigentes, y el compromiso de actuar de conformidad con el derecho internacional, incluida la Carta en su totalidad, así como con las normas de comportamiento responsable de los Estados en el ciberespacio. Nos comprometemos a promover y hacer progresar la paz y la estabilidad en el ciberespacio mediante debates y en foros como el actual grupo de trabajo de composición abierta.

En este contexto, y en consonancia con nuestro apoyo a la labor del grupo de trabajo de composición abierta, la Unión Europea no estaba en condiciones de respaldar la resolución 78/237, titulada “Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional”, aprobada por la Asamblea General el 22 de diciembre de 2023.

La Unión Europea considera que la resolución podría haber representado mejor el frágil consenso alcanzado en el grupo de trabajo de composición abierta, sus procesos precedentes y las resoluciones consensuadas anteriores.

Principalmente, la resolución no hace referencia al marco acumulativo y evolutivo de comportamiento responsable de los Estados en el uso de las TIC, un marco que es el resultado de más de 20 años de negociaciones y que ha sido respaldado repetidamente por consenso por la Asamblea General.

En su lugar, destaca, especialmente en el párrafo 5 y el párrafo 16 del preámbulo, propuestas sustantivas concretas respaldadas por un pequeño grupo de Estados, que la Unión Europea teme que puedan obstaculizar el planteamiento progresivo y basado en el consenso gracias al cual el grupo de trabajo de composición abierta ha podido avanzar en los últimos años.

La Unión Europea y sus Estados miembros consideramos que la aplicación del marco de las Naciones Unidas de comportamiento responsable de los Estados en el uso de las TIC es de suma importancia para garantizar un entorno abierto, seguro, estable, accesible y pacífico para las TIC, y nos preocupa ver que esta resolución se basa en un texto no consensuado que podría llevar a reinterpretar la labor del grupo de trabajo de composición abierta y los documentos consensuados existentes.

La Unión Europea sigue totalmente decidida a encontrar elementos comunes que permitan avanzar hacia el consenso en el actual grupo de trabajo de composición abierta, y respalda plenamente las iniciativas colectivas encaminadas a diseñar un mecanismo inclusivo, permanente y orientado a la acción para establecer un diálogo institucional periódico cuando el actual grupo de trabajo de composición abierta concluya su labor.

**Sobre las solicitudes relacionadas con el párrafo 8 de la resolución**

Se ha avanzado mucho en el debate sobre un futuro mecanismo, una vez que concluya la labor del grupo de trabajo de composición abierta 2021-2025. El informe del Secretario General (A/78/76), encargado por la Asamblea General en su resolución 77/37, incluía observaciones y conclusiones sobre el alcance, la estructura, los principios, el contenido, los preparativos y las modalidades para el establecimiento del programa de acción para promover el comportamiento responsable de los Estados en el uso de las tecnologías de la información y las comunicaciones en el contexto de la seguridad internacional. Además, el grupo de trabajo de composición abierta 2021-2025 acordó elementos comunes para un futuro mecanismo de diálogo institucional periódico en su informe anual de 2023 sobre los progresos realizados. Por último, la Presidencia del grupo de trabajo de composición abierta 2021-2025 ha propuesto otros elementos comunes en un documento de debate,

a partir de las propuestas de las delegaciones y las discusiones de del sexto período de sesiones sustantivo del grupo de trabajo de composición abierta.

Teniendo en cuenta los avances logrados en la determinación de los elementos comunes del futuro mecanismo, la Unión Europea seguirá expresando su opinión sobre un futuro mecanismo de diálogo institucional periódico.

El fomento de la seguridad y la estabilidad internacionales en el ciberespacio y la mejora del conocimiento y la aplicación del marco de las Naciones Unidas de comportamiento responsable de los Estados en el ciberespacio deben seguir siendo prioridades del diálogo institucional periódico sobre estas cuestiones bajo los auspicios de las Naciones Unidas.

En respuesta al llamamiento para establecer un diálogo institucional permanente, inclusivo y transparente, con una participación amplia, bajo los auspicios de las Naciones Unidas, tal como se articula en los informes de 2021 del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Comunicaciones en el Contexto de la Seguridad Internacional y el Grupo de Expertos Gubernamentales, el programa de acción, una propuesta iniciada por un grupo interregional de países[1], representa una oportunidad para presentar una estructura permanente de diálogo institucional periódico en las Naciones Unidas y, por tanto, permitir a la comunidad internacional centrar sus debates en la sustancia en lugar de tener discusiones recurrentes sobre futuros procesos. En este contexto, el programa podría convertirse en el mecanismo evolutivo de la futura cooperación en el seno de la Primera Comisión de la Asamblea General.

Con este fin, el planteamiento colectivo debe centrarse en tratar de encontrar un equilibrio entre dos aspectos igualmente importantes de nuestro trabajo: la aplicación del marco establecido de comportamiento responsable de los Estados en el uso de las TIC en el contexto de la seguridad internacional, y el desarrollo ulterior del marco. El desarrollo del marco se basa, entre otras cosas, en las enseñanzas extraídas de la aplicación de los compromisos vigentes.

El mecanismo debe ser inclusivo, estar orientado a la acción y proporcionar una plataforma para debates e intercambios detallados, facilitar la creación de capacidad y permitir el desarrollo ulterior del marco normativo y su actualización de acuerdo con la evolución en curso del entorno de las TIC sobre la base del consenso.

También debe permitir la participación oficial de las partes interesadas pertinentes y las consultas con ellas, incluidos el sector privado, el mundo académico y la sociedad civil, para que puedan estudiarlo y aportar sus perspectivas y conocimientos especializados únicos sobre las cuestiones pertinentes. Ello centrará aún más los esfuerzos en ayudar a los Estados a promover la aplicación del marco de comportamiento responsable de los Estados y la creación de capacidades en función de las necesidades para aumentar la ciberresiliencia tanto a nivel nacional como mundial.

El programa de acción debe basarse en el marco normativo que figura en los sucesivos informes de consenso del Grupo de Expertos Gubernamentales y el grupo de trabajo de composición abierta, así como en los compromisos y medidas resultantes. El futuro mecanismo debe convocar conferencias periódicas de examen cada varios años (por ejemplo, cada tres o cuatro años) para examinar el marco de comportamiento responsable de los Estados, actualizarlo en caso necesario y proporcionar orientación estratégica para el trabajo del mecanismo.

[1] Véase https://documents.unoda.org/wp-content/uploads/2021/11/Working-paper-on-the-proposal-for-a-Cyber-PoA.pdf.

El programa de acción podría celebrar períodos de sesiones oficiales anuales, en los que se podría examinar la labor llevada a cabo en los debates detallados abiertos a lo largo del año. En los períodos de sesiones oficiales anuales se podría decidir la creación de reuniones técnicas abiertas, grupos de trabajo o líneas de trabajo a fin de centrarse en cuestiones prioritarias específicas para avanzar en el programa.

La participación en las líneas de trabajo técnicas debe ser voluntaria y estar abierta a todos los Estados. La configuración de las líneas de trabajo, incluidas la participación de las partes interesadas y la frecuencia de las reuniones, debe decidirse en las reuniones anuales o en las conferencias de examen. Estas reuniones deben orientarse hacia la elaboración de un documento final que contenga conclusiones operacionales basadas en las enseñanzas extraídas de la aplicación del marco de comportamiento responsable de los Estados, en un ciclo de mejora continua.

El programa de acción también podría potenciar la participación regional mediante la cooperación con organizaciones regionales para aprovechar las iniciativas pertinentes existentes y las estructuras y plataformas de creación de capacidad existentes. Estos esfuerzos colectivos ayudarían a los países a articular y recibir la creación de capacidad necesaria. Si bien se hace hincapié en la responsabilidad primordial de los Estados en el mantenimiento de la paz y la seguridad internacionales y en su función crucial en el programa de acción, debe potenciarse el intercambio y la colaboración con las partes interesadas proporcionando un lugar de participación inclusiva y significativa.

En cuanto a los trabajos preparatorios y el establecimiento del programa de acción, en 2024 y 2025 deben organizarse reuniones entre períodos de sesiones y reuniones específicas del grupo de trabajo de composición abierta para seguir profundizando en los diferentes aspectos del programa de acción, incluidas las consecuencias presupuestarias relacionadas con el mecanismo permanente y la identificación de los agentes pertinentes dentro de las Naciones Unidas para desempeñar estas funciones. Los resultados de estas sesiones deben reflejarse en los respectivos informes anuales sobre los progresos realizados por el grupo de trabajo de composición abierta. El programa de acción debe estar operativo una vez que concluya la labor del grupo de trabajo de composición abierta 2021-2025.