**COMITÉ INTERAMERICANO CONTRA EL TERRORISMO (CICTE)**

QUINTA REUNIÓN DEL GRUPO DE TRABAJO OAS/Ser.L/X.5

SOBRE COOPERACIÓN Y MEDIDAS DE FOMENTO CICTE/GT/MFCC/doc.14/24

DE LA CONFIANZA EN EL CIBERESPACIO 18 abril 2024

26 y 27 de febrero de 2024 Original: inglés

Washington, D. C., Estados Unidos

INFORME DE LA QUINTA REUNIÓN DEL GRUPO DE TRABAJO SOBRE COOPERACIÓN Y MEDIDAS DE FOMENTO DE LA CONFIANZA EN EL CIBERESPACIO

(Preparado por la Secretaría del CICTE)

INFORME DE LA QUINTA REUNIÓN DEL GRUPO DE TRABAJO SOBRE COOPERACIÓN Y MEDIDAS DE FOMENTO DE LA CONFIANZA EN EL CIBERESPACIO

(Preparado por la Secretaría del CICTE)

**Introducción**

De conformidad con la resolución [CP/RES. 1245 (2480/24),](http://scm.oas.org/doc_public/SPANISH/HIST_24/CP49022S03.docx) la Quinta Reunión del Grupo de Trabajo sobre Cooperación y Medidas de Fomento de la Confianza en el Ciberespacio (GT-MFCC) se celebró en la Sede de la OEA en Washington DC los días 26 y 27 de febrero de 2024. Los Estados Miembros que participaron en la reunión fueron los siguientes: Antigua y Barbuda, Argentina, Bahamas, Bolivia, Brasil, Canadá, Chile, Colombia, Costa Rica, Dominica, República Dominicana, Ecuador, El Salvador, Granada, Guyana, Jamaica, México, Panamá, Perú, San Cristóbal y Nieves, San Vicente y las Granadinas, Uruguay y Estados Unidos de América. Todos los documentos de la reunión están disponibles en: https://www.oas.org/ext/en/main/calendar/event/id/140

[https://www.oas.org/ext/en/main/calendar/event/id/140](https://www.oas.org/ext/es/principal/calendario/evento/id/140)

**Sesión de apertura**

La reunión fue inaugurada por Jennifer Bachus, Subsecretaria Principal Adjunta de la Oficina de Política Cibernética y Digital del Departamento de Estado de Estados Unidos. La Sra. Bachus destacó las contribuciones del Grupo de Trabajo en la formulación y aprobación de las medidas de fomento de la confianza cibernética en la región de la OEA. Señaló que los esfuerzos del Grupo de Trabajo promovían el marco de las Naciones Unidas para garantizar un ciberespacio más seguro y promover la paz y la seguridad en la región.

El Embajador Claudio Peguero, Asesor en Asuntos Cibernéticos del Ministerio de Relaciones Exteriores de la República Dominicana y Vicepresidente del Grupo de Trabajo sobre Cooperación y Medidas de Fomento de la Confianza en el Ciberespacio, subrayó la importancia de la aplicación de las medidas de fomento de la confianza para fortalecer la cooperación entre los Estados Miembros. También destacó la labor del grupo en el establecimiento de un marco para el intercambio de información, el desarrollo de una mayor capacidad y la adopción de prácticas que promovieran la confianza y la estabilidad en el ciberespacio. Hizo hincapié en que la ciberseguridad se ha convertido en un desafío fundamental que requiere una respuesta colectiva y coordinada.

Ivan C. Marques, Secretario de Seguridad Multidimensional de la Organización de los Estados Americanos, también pronunció un discurso de apertura. Señaló que el Grupo de Trabajo apoya la labor de las Naciones Unidas, en particular los Grupos de Expertos Gubernamentales de las Naciones Unidas sobre el Desarrollo en el Ámbito de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional y el Grupo de Trabajo de composición abierta de las Naciones Unidas sobre seguridad cibernética (OEWG por sus siglas en inglés). Reafirmó el compromiso constante de la OEA de apoyar a los Estados Miembros en la aplicación de las once (11) medidas de fomento de la confianza ya acordadas por el Grupo de Trabajo de MFCC durante sus cuatro (4) reuniones anteriores.

**Primera sesión plenaria**

Liesyl Franz, Subsecretaria Adjunta de Seguridad Cibernética Internacional de la Oficina de Política Cibernética y Digital del Departamento de Estado de Estados Unidos, presidió el Grupo de Trabajo.

Durante la primera sesión plenaria, las delegaciones examinaron y aprobaron, sin modificaciones, el proyecto de programa y el proyecto de calendario de la reunión.

**Segunda sesión plenaria**

El Presidente comenzó refiriéndose a las cinco medidas de fomento de la confianza (MFC) convenidas durante la cuarta reunión del Grupo de Trabajo y acogiendo con satisfacción las nuevas propuestas para mejorar la aplicación de las medidas existentes. El Presidente también se refirió a las medidas de fomento de la confianza que se estaban debatiendo a nivel mundial, incluidas las medidas de fomento de la confianza en los puntos de contacto, y alentó a los Estados miembros de la OEA a que apoyaran los esfuerzos de las Naciones Unidas a este respecto.

Kerry-Ann Barrett, gerente del Programa de Ciberseguridad del CICTE, informó sobre las actividades realizadas entre 2022 y 2024 para implementar las medidas de fomento de la confianza cibernéticas aprobadas. Entre otras cosas, informó que actualmente 89 Contactos de Política Cibernética y 19 Contactos del Ministerio de Relaciones Exteriores de 30 Estados Miembros de la OEA tienen acceso al portal interno del Grupo de Trabajo. También destacó dos iniciativas recientes del CICTE: (1) la alineación de los cursos de ciberdiplomacia y derecho internacional del CICTE con temas relacionados con las medidas de fomento de la confianza aprobadas y (2) un prototipo para mejorar los servicios del Portal del Grupo de Trabajo.

Mariana Jaramillo, Oficial del Programa de Seguridad Cibernética, luego presentó el plan de trabajo propuesto para 2024, que incluye actividades para actualizar el portal; lanzar una nueva serie de webinarios sobre las MFC aprobadas; y continuar la alineación de las iniciativas existentes y nuevas de creación de capacidad del CICTE con las MFC aprobadas. La presentación concluyó con los resultados de la encuesta voluntaria sobre la aplicación de las medidas de fomento de la confianza.

Las delegaciones de Argentina, Bahamas, Canadá, Chile, Colombia, Costa Rica, Dominica, Ecuador, El Salvador, Guyana, México, Perú y los Estados Unidos hicieron uso de la palabra para formular observaciones o dar las gracias a la Secretaría del CICTE.

**Tercera sesión plenaria[[1]](#footnote-2)**

A continuación, los Estados miembros ofrecieron actualizaciones sobre sus políticas de ciberseguridad, experiencias recientes relacionadas con la ciberseguridad y lecciones aprendidas en materia de creación de capacidades cibernéticas:

* *Canadá* mencionó la reciente enmienda de su Ley de protección de los sistemas cibernéticos críticos que establecía un marco reglamentario para la notificación de incidentes al Gobierno y mecanismos para prevenir las actividades maliciosas que afectaran a las infraestructuras críticas nacionales. Canadá también ha designado un perfil de política cibernética digital y un representante para seguir integrando la política cibernética a nivel nacional y mundial. Canadá también se refirió al Proceso de Pall Mall patrocinado por los Gobiernos de Francia y el Reino Unido que tenía por objeto hacer frente a los peligros derivados del ecosistema de la capacidad comercial de intrusión cibernética, e invitó a las delegaciones interesadas a participar en el proceso.
* *Chile* proporcionó una visión general de su Política Nacional de Seguridad Cibernética (2023-2028) y plan de implementación publicados recientemente, que, entre otras cosas, aborda la aplicación del derecho internacional en el ciberespacio, incluido el derecho de los derechos humanos; la importancia de la diplomacia cibernética; la inteligencia artificial; la delincuencia organizada; las perspectivas de género y las cuestiones relacionadas con la ciberdefensa. Chile expresó la necesidad de contar con conocimientos jurídicos especializados en materia de derecho internacional aplicable en el ciberespacio a fin de hacer frente con mayor eficacia a las actividades de ciberdelincuencia.
* *Colombia* compartió que actualmente está actualizando sus políticas digitales, incluida una nueva Estrategia Nacional de Ciberseguridad, y está estableciendo un departamento de ciberseguridad. Colombia identificó desafíos para abordar los riesgos cibernéticos, como el alto costo que implican, la naturaleza cambiante de las amenazas y la dificultad de atribuir acciones maliciosas. Por otra parte, Colombia hizo hincapié en la necesidad de crear capacidades de ciberseguridad, mejorar la infraestructura de seguridad, implementar la gestión de riesgos y reducir la brecha digital, evitando al mismo tiempo la duplicación de esfuerzos. Colombia destacó sus esfuerzos para impartir cursos de ciberdiplomacia a diplomáticos.
* *Estados Unidos* informó del lanzamiento de una nueva Estrategia Nacional de Ciberseguridad, que llama a reequilibrar la responsabilidad de defender el ciberespacio hacia los actores más capaces y realinear los incentivos para favorecer las inversiones a largo plazo en seguridad. Los Estados Unidos también tomaron nota de la publicación de su Estrategia Nacional de Ciberfuerza de Trabajo y Educación y señalaron que las inversiones en personas, procesos y tecnología eran esferas de creación de capacidad que se reforzaban mutuamente. Los Estados Unidos expresó su disposición a colaborar en el desarrollo de capacidades cibernéticas y mencionó una próxima Estrategia Internacional del Ciberespacio y las Tecnologías Digitales.
* *El Salvador* expresó su objetivo de convertirse en un centro tecnológico en la región de la OEA. El Salvador subrayó los progresos realizados en el establecimiento de un marco jurídico y normativo para promover las capacidades cibernéticas y abordar las vulnerabilidades en la infraestructura crítica y los recursos de información nacionales, incluida una estrategia nacional de seguridad cibernética. El Salvador también destacó la legislación reciente, como la Ley de promoción de la innovación y la fabricación tecnológica, y una Declaración conjunta sobre prioridades compartidas en la política digital, emitida recientemente por El Salvador y los Estados Unidos.
* *Argentina* destacó su nueva Estrategia Nacional de Seguridad Cibernética, elaborada conjuntamente con el sector privado. La estrategia nacional de respuesta se ocupa de los protocolos de respuesta a incidentes, la observancia de las normas internacionales y la coordinación con otros procesos multilaterales.
* *Brasil* destacó su nueva Estrategia Nacional de Seguridad Cibernética y el desarrollo de un nuevo marco legal, junto con la creación de directrices y folletos accesibles a través de los sitios web oficiales de los ministerios. Además, el Brasil está capacitando a los funcionarios públicos sobre estas cuestiones y participando activamente en diversos foros internacionales como el BRIC, el MERCOSUR, la OEA y el GTCA.
* *Costa Rica* informó sobre el desarrollo de su Segunda Estrategia Nacional de Seguridad Cibernética, que designaba la seguridad cibernética como una prioridad nacional y tenía por objeto mejorar su seguridad digital.
* *México* señaló que seguía incorporando normas internacionales sobre seguridad cibernética adaptándolas al contexto mexicano, al tiempo que destacó la necesidad de promover la cooperación y el diálogo con los asociados internacionales. México destacó la creciente fragmentación del diálogo y los procesos multilaterales, y destacó la necesidad de una perspectiva más amplia entre esos foros. México destacó la importancia de normalizar los marcos legislativos para aumentar la resiliencia y proteger las infraestructuras críticas y los sistemas de información. México señaló que el desarrollo de la capacidad había sido fundamental para superar las limitaciones de recursos.
* La *República Dominicana* subrayó la importancia de aplicar las medidas de fomento de la confianza cibernética aprobadas. La República Dominicana describió los progresos realizados en el desarrollo y la aplicación de su Estrategia Nacional de Seguridad Cibernética y mencionó que estaba pendiente de aprobación una nueva ley de seguridad cibernética. La República Dominicana destacó la integración de la ciberseguridad en su Estrategia de Inteligencia Artificial, haciendo hincapié en ocho principios, incluido el respeto de los derechos humanos. La República Dominicana busca establecerse como un centro de capacitación en ciberseguridad y ha nombrado un embajador cibernético, el primero en la región de América Latina y el Caribe.
* *Ecuador* informó sobre la creación de un comité de ciberseguridad centrado en el entorno digital. Con la asistencia técnica del CICTE, el Ecuador elaboró su Estrategia Nacional de Seguridad Cibernética. El Ecuador ha venido colaborando con Cyber4Dev y CyberNet y es un centro subregional para la región andina, designada por Estonia. El Ecuador señaló que los Estados Unidos habían apoyado su participación en foros internacionales y mejorado su resiliencia en materia de seguridad cibernética a nivel nacional. Ecuador también destacó la participación en varios programas del CICTE, incluido el Cyber Women Challenge y She Secures.
* *Uruguay* destacó la creación de un CERT nacional como parte de su nueva Agenda Digital. Además de supervisar las actividades cibernéticas de más de diez organismos nacionales, el Uruguay ha centrado sus esfuerzos en la creación de capacidad mediante programas académicos y la capacitación de técnicos de seguridad cibernética, lo que ha dado lugar a la creación de un programa nacional de estudios sobre seguridad cibernética para escuelas públicas y privadas.
* *Bolivia* está trabajando activamente en un marco jurídico de seguridad cibernética, incluido el desarrollo de una ley para la protección de datos personales. Adicionalmente, Bolivia ha establecido un sistema de registro de incidentes en todas las entidades públicas y ha proporcionado pautas para que estas entidades sigan al abordar las preocupaciones de seguridad cibernética.
* *Las Bahamas* están redactando actualmente una legislación sobre seguridad cibernética que tiene por objeto establecer, entre otras cosas, una nueva agencia de seguridad cibernética. También está trabajando en la publicación de una Estrategia Nacional de Ciberseguridad, cuya aplicación estará dirigida por el Equipo de Respuesta a Incidentes Cibernéticos (CIRT). Además, las Bahamas están revisando su legislación sobre protección de datos y han emprendido numerosas actividades de fomento de la capacidad con diversos interesados. El país recientemente llevó a cabo su primer simulacro cibernético y acogió el Simposio Anual de Ciberseguridad del CICTE para ayudar a crear una mayor conciencia y capacidad de los interesados en la seguridad cibernética.

**Cuarta sesión plenaria**

Se celebró una mesa redonda sobre el tema “Promoción de la aplicación de las medidas de fomento de la confianza en el hemisferio occidental”.

* *Pablo A. Castro, Coordinador de Seguridad Cibernética, División de Seguridad Internacional y Humana, Ministerio de Relaciones Exteriores, Chile,* señaló el papel crítico de la Secretaría del CICTE en el apoyo a los Estados Miembros, particularmente en la implementación de medidas de fomento de la confianza cibernética a través del desarrollo de capacidades. Destacó la necesidad de que los Estados y otros interesados siguieran intercambiando las mejores prácticas. Castro sugirió formalizar este compromiso, potencialmente a través de reuniones estructuradas con otros Estados miembros, y propuso el desarrollo de un plan de implementación para las once medidas de fomento de la confianza para orientar la acción colectiva. Reconociendo que los Estados miembros tienen distintos niveles de madurez en materia de ciberseguridad, el Sr. Castro subrayó la importancia de la cooperación regional. Destacó además la nueva Estrategia Nacional de Seguridad Cibernética de Chile, que incluye una estrategia para la cooperación internacional y la participación del sector privado. El Sr. Castro también subrayó la importancia de compartir experiencias regionales en foros internacionales como el Grupo de Trabajo de composición abierta de las Naciones Unidas.
* *Daniela Ruiz Domínguez, Directora de Ciberseguridad y Armas Convencionales de la Secretaría de Relaciones Exteriores de México,* señaló las crecientes tensiones en otras regiones con respecto al uso malintencionado de las tecnologías de la información y la comunicación por parte de los actores estatales y las tensiones relacionadas en el ciberespacio. Señaló además que esas tendencias podían afectar a la región de la OEA y alentó al Grupo de Trabajo a que las abordara. Subrayó que el Grupo de Trabajo servía de plataforma para intercambiar información, proporcionar recursos para las mejores prácticas, realizar ejercicios conjuntos y facilitar sesiones de capacitación conjuntas. La Sra. Domínguez acogió con satisfacción la encuesta sobre la aplicación propuesta por la Presidencia, señalando la importancia de compartir los desafíos a que se enfrentaba cada país y de trabajar eficazmente con el sector privado en general.
* *Muriana McPherson, Directora de la Autoridad Nacional de Gestión de Datos de Guyana,* hizo hincapié en que la verificación y aplicación de las medidas de fomento de la confianza podía requerir mucha mano de obra, en particular para los países menos adelantados, y propuso que se aumentara el intercambio de información en el portal entre los puntos de contacto. La Sra. McPherson señaló que Guyana tenía un proyecto de Estrategia Nacional de Seguridad Cibernética y una legislación sobre la ciberdelincuencia que se ajustaban en gran medida a la Convención de Budapest, así como una legislación sobre asistencia judicial recíproca. Además, en 2023 se adoptó una Ley de Protección de Datos. Guyana también tiene un equipo de respuesta a incidentes cibernéticos y un esquema nacional de seguridad cibernética para compartir información entre instituciones públicas en caso de un incidente cibernético. Se han puesto en marcha planes para modificar la legislación relativa a la notificación de ciberincidentes, con un seguimiento de la red gubernamental 24 horas al día, 7 días a la semana. La Sra. McPherson señaló que más del 75% de los ministerios de Guyana habían recibido capacitación en materia de sensibilización, y más de 50 personas habían recibido capacitación para capacitar a otros. La Sra. McPherson destacó la importancia de contar con un defensor de alto nivel para apoyar estos esfuerzos, citando el apoyo del Primer Ministro a su primera evaluación de riesgos cibernéticos realizada el año pasado.
* *Claudio Peguero, Embajador, Asesor en Asuntos Cibernéticos, Ministerio de Relaciones Exteriores, República Dominicana,* destacó la adopción de su país de una Estrategia Nacional de Seguridad Cibernética y la designación de un Embajador Cibernético. También destacó que la República Dominicana está creando capacidad de diplomacia cibernética, dando prioridad a la integración de una perspectiva de género, así como a la capacidad para fortalecer la infraestructura crítica. El Embajador Peguero destacó la participación de diversos actores, incluido el sector privado, en el desarrollo de proyectos relacionados con la legislación, las comunicaciones y la infraestructura de ciberseguridad. También afirmó que la República Dominicana había promulgado un decreto presidencial que preveía la denuncia de incidentes y la divulgación responsable de las vulnerabilidades.

Las delegaciones de Argentina, Chile, Colombia, Estados Unidos y Uruguay hicieron uso de la palabra para reflexionar sobre las presentaciones realizadas y formular observaciones sobre la labor del Grupo de Trabajo sobre medidas de fomento de la confianza, en particular su papel en los debates del Grupo de Trabajo de composición abierta de las Naciones Unidas.

**Quinta sesión plenaria**

Se celebró una segunda mesa redonda sobre el tema “Fomento y promoción de la inclusión, el liderazgo y la participación efectiva y significativa de la mujer en los procesos de adopción de decisiones relacionados con las tecnologías de la información y las comunicaciones”.

* *Julia Rodríguez Acosta, Ministra Consular, Misión Permanente de El Salvador ante las Naciones Unidas, El Salvador,* señaló el reconocimiento de las experiencias diferenciadas en línea entre mujeres y hombres y la importancia de crear entornos en línea más seguros. Dada la función de las mujeres en la paz y la seguridad internacionales, la Sra. Rodríguez destacó la importancia de desarrollar la capacidad de las mujeres en materia de ciberseguridad, incluido el apoyo a los programas STEM y la promoción de la inclusión de género en general.
* *Belén Gallardo, Asesora de Políticas de Programas de la División Internacional de Política Cibernética de Global Affairs Canada,* destacó el compromiso de Canadá de promover la igualdad de género a través de iniciativas de política interna y externa, incluso en el contexto de la asistencia internacional para el desarrollo. A nivel nacional, se están realizando esfuerzos para incorporar la perspectiva de género en las cuestiones relacionadas con la seguridad cibernética, como el marco nacional de seguridad cibernética (NCS) y la agenda de mujeres, paz y seguridad. La Sra. Gallardo mencionó el apoyo del Canadá a la Beca Mujeres en la Ciberseguridad (WiC), un programa que facilita la participación de más de 200 diplomáticas y expertas de diversas regiones en actos como el Grupo de Trabajo de composición abierta (OEWG). Además, destacó la colaboración de Canadá con el CICTE para abordar la violencia de género en línea, y con la Comisión Interamericana de Mujeres (CIM) para desarrollar legislación modelo y aumentar la conciencia regional sobre la sensibilidad de género en la ciberseguridad.
* *Lisa Sharland, investigadora principal y directora del Programa de Protección de Civiles y Seguridad Humana, The Stimson Center* identificó las barreras que normalmente impiden que las mujeres participen en las discusiones cibernéticas, como la falta de habilidades, responsabilidades de cuidado y otros factores sistémicos. Sharland indicó que abordar las cuestiones de género es una responsabilidad compartida (no solo responsabilidad de las mujeres), y que las políticas de seguridad cibernética deben abordar de manera efectiva la desinformación de género y el impacto de género de los incidentes cibernéticos. Además, destacó la importancia de considerar la protección de los derechos humanos, especialmente en lo que respecta a la forma en que se cuantifican los conjuntos de datos. Además, abordar la desinformación de género, la radicalización en línea y garantizar la rendición de cuentas por los comportamientos en línea son componentes cruciales para promover la ciberseguridad inclusiva de género.

Las delegaciones de Argentina, Chile, Colombia, Ecuador y Estados Unidos hicieron uso de la palabra para alentar y promover la inclusión, el liderazgo y la participación efectiva y significativa de la mujer en los procesos de adopción de decisiones relacionados con las tecnologías de la información y las comunicaciones. En particular, las beneficiarias del programa de becas Mujeres en Seguridad Cibernética (WiC) reconocieron que el programa desempeñaba un papel importante en el aumento de la participación de su país en los procesos de las Naciones Unidas.

**Quinta sesión plenaria**

La mañana del 27 de febrero de 2024 se abrió con el panel de discusión “Explorando el desarrollo de posiciones nacionales sobre la aplicabilidad del derecho internacional al ciberespacio”.

* *Gary Corn, Director de Programa y Profesor Adjunto, Tecnología, Derecho y Seguridad, American University Washington College of Law,* reflexionó sobre los temas relacionados con la aplicabilidad del derecho internacional al ciberespacio. Entre otros puntos, destacó que tanto los estados como los actores no estatales a menudo están involucrados en el ciberespacio, y algunos participan en situaciones consideradas como «conflictos armados». En consecuencia, es necesario elaborar normas adecuadas para abordar estos diferentes escenarios y agentes en el ámbito del ciberespacio y que otras normas existentes en virtud del derecho internacional puedan ser útiles a este respecto. También mencionó las complejidades del área de los efectos cibernéticos, que implica el uso de herramientas cibernéticas para influir en los espacios de información, incluida la desinformación y la propaganda.
* *Kimberley Raleigh, Asesora Principal de Políticas, Oficina de Política Cibernética y Digital, Departamento de Estado de los Estados Unidos,* indicó que los estados deben redactar posiciones nacionales con respecto a la aplicabilidad del derecho internacional en el ciberespacio. Sin esas posiciones, es difícil para otros Estados entender dónde se trazan las líneas rojas y evitar cruzarlas. El Compendio de contribuciones nacionales voluntarias sobre el tema del derecho internacional y el ciberespacio[[2]](#footnote-3) tiene por objeto promover la transparencia y fomentar la confianza entre los Estados. El desarrollo de una posición nacional implica la consolidación de opiniones entre diferentes organismos gubernamentales, incluidos los de defensa, relaciones exteriores, justicia, inteligencia y seguridad nacional. La Sra. Raleigh destacó la importancia de que los expertos participaran en las operaciones cibernéticas y en el derecho internacional durante el proceso de redacción.
* *Marcela Zamora Ovares, Jefa del Departamento de Desarme, Terrorismo y Delincuencia Organizada de la Dirección General de Política Exterior de Costa Rica.* En respuesta al ciberataque de 2021 a los servicios públicos, Costa Rica reforzó sus capacidades de respuesta a incidentes y ciberseguridad, en particular en lo que respecta a los datos de ciudadanos y estados. La Sra. Zamora destacó la importancia de integrar el derecho internacional, incluido el derecho de los derechos humanos, en los marcos de seguridad cibernética. El desarrollo de una posición nacional sobre el derecho internacional en el ciberespacio también puede promover el crecimiento económico. La Sra. Zamora compartió la experiencia de Costa Rica en la consulta de diversos recursos, como el Manual de Tallin, para elaborar su posición nacional.
* *El Dr. Andraz Kastelic, del Programa de Seguridad y Tecnología del Instituto de las Naciones Unidas de Investigación sobre el Desarme (UNIDIR),* presentó los desafíos que pueden existir en el desarrollo de posiciones nacionales sobre el derecho internacional en el ciberespacio, incluida la falta de conciencia y capacidad. El UNIDIR tiene el mandato de ayudar a los Estados de las Naciones Unidas a formular y articular posiciones nacionales sobre la forma en que el derecho internacional se aplica a la conducta de los Estados en el ciberespacio y, por lo tanto, ofrece actividades de creación de capacidad, como talleres basados en escenarios para asesores jurídicos. Además, el UNIDIR lleva a cabo investigaciones y proporciona orientación sobre este tema.

Las delegaciones de Argentina, Brasil, Canadá, Chile, Colombia, Costa Rica, Dominica, Granada, Ecuador, El Salvador, Santa Lucía y Estados Unidos reflexionaron sobre el desarrollo de posiciones nacionales sobre la aplicabilidad del derecho internacional al ciberespacio, y se refirieron a las cuestiones de soberanía que pueden estar involucradas en dicho proceso, incluida la incapacidad de atribuir cuando los ataques se realizan a través de apoderados.

**Séptima sesión plenaria**

La presentación sobre el Esquema de Gravedad de Incidentes Cibernéticos de Patrick Kyhos, Director de Operaciones y Respuesta a Incidentes de la Oficina del Director Nacional de Ciberseguridad de la Casa Blanca, fue eliminada de la agenda debido a un conflicto de programación.

**Octava sesión plenaria**

Los Estados miembros discutieron cómo aprovechar el directorio existente de puntos de contacto (POC) del CBMS con el Directorio Global POC de las Naciones Unidas:

* *Estados Unidos* mencionó que en las deliberaciones del Grupo de Trabajo de composición abierta se había reconocido la importancia de la coherencia entre los directorios regionales y el directorio mundial y sugirieron que tal vez fuera apropiado que el Grupo de Trabajo examinara esta cuestión ahora, mientras el directorio de los centros de coordinación de las Naciones Unidas todavía se estaba elaborando (y no después de su creación). Estados Unidos también enfatizó la importancia de mantener información consistente en ambas plataformas y sugirió la adopción de una práctica en la que los Estados miembros de la OEA que deseen nominar a la(s) misma(s) persona(s) para el directorio POC de la ONU que sean POCs de la OEA actuales podrían autorizar expresamente al CICTE a transmitir esos datos de contacto a la ONU. Los Estados Unidos también propusieron que el CICTE realizara actualizaciones periódicas de la red de centros de coordinación de las medidas de fomento de la confianza para garantizar que la información se mantuviera actualizada, posiblemente mediante invitaciones periódicas para actualizar la información de los centros de coordinación de las medidas de fomento de la confianza.
* *Chile* comentó la puesta en marcha de los programas de trabajo del Grupo de Trabajo sobre las medidas de fomento de la confianza y apoyó la propuesta de la secretaría del CICTE de acoger seminarios web entre los programas de trabajo para facilitar la comunicación y la participación entre los Estados Miembros. Chile también señaló la necesidad de seguir debatiendo la creación del directorio mundial de las Naciones Unidas. Además, Chile sugirió que los Estados Miembros pudieran elegir si el CICTE debía enviar información sobre el Programa de Cooperación a las Naciones Unidas o si los países debían hacerlo ellos mismos.
* *México* sugirió la posibilidad de que los países asignaran los mismos programas de actividades al Grupo de Trabajo sobre las medidas de fomento de la confianza que al directorio mundial de las Naciones Unidas. México enfatizó los beneficios de tener funcionarios familiarizados con la dinámica de este directorio PoC regional, lo que los ayudaría a aprovechar las mejores prácticas, optimizar los procesos y evitar la duplicación de tareas. México también expresó su disposición a permitir que los países decidan si comparten o no su información del PoC para el directorio global a través del CICTE.
* *Brasil* alentó a una mayor sinergia entre las dos redes y alentó a la Secretaría del CICTE a que siguiera atenta a la evolución de la cuestión en las Naciones Unidas.
* *Colombia* también señaló la importancia de una mayor sinergia para facilitar la coordinación y sugirió que se siguiera examinando la cuestión por conducto del Grupo de Trabajo.

**Elección de las autoridades**

A continuación, la reunión procedió a la elección de los miembros de la Mesa del Sexto Grupo de Trabajo sobre Cooperación y Medidas de Fomento de la Confianza en el Ciberespacio.

La delegación de Chile designó al Gobierno de la República Dominicana para presidir la Sexta Reunión del Grupo de Trabajo y la moción fue aprobada por aclamación. El Embajador Claudio Peguero, Asesor en Asuntos Cibernéticos del Ministerio de Relaciones Exteriores de la República Dominicana, aceptó la nominación en nombre de su país y expresó el agradecimiento de su gobierno por la confianza otorgada.

A continuación, la delegación de Colombia presentó la candidatura del Gobierno del Canadá para el cargo de Vicepresidente. La propuesta también fue aprobada por aclamación. La Sra. Belén Gallardo, Asesora de Políticas de Programas de la División de Política Cibernética Internacional de Global Affairs Canada, aceptó la candidatura en nombre de su Gobierno.

**Sesión de cierre**

La Presidencia agradeció a todos los delegados su participación y resumió las principales propuestas formuladas durante la reunión:

1. Elaboración de programas de formación para las academias diplomáticas en los Estados miembros de la OEA;
2. Elaboración de un plan de trabajo regional para apoyar la aplicación de las medidas de fomento de la confianza cibernética acordadas por la OEA;
3. Celebración de reuniones oficiosas del Grupo de Trabajo de la OEA sobre las medidas de fomento de la confianza en las Naciones Unidas antes de los períodos de sesiones del Grupo de Trabajo de composición abierta;
4. Organización de mesas redondas para ayudar a los Estados miembros a desarrollar posiciones nacionales sobre la aplicabilidad del Derecho internacional al ciberespacio;
5. Promoción de sinergias entre el Directorio de Centros de Operaciones de la OEA y el Directorio de Centros de Operaciones de las Naciones Unidas.

Al no haber otros asuntos que debatir, la sesión se levantó a las 12.45 horas.

cicte01702s01

1. La delegación del Brasil señaló la falta de interpretación en los cuatro (4) idiomas oficiales de la OEA, lo que repercutía negativamente en la plena participación de todos los Estados Miembros. La Secretaría del CICTE respondió que históricamente las reuniones del Grupo de Trabajo se han celebrado sólo en español e inglés debido a limitaciones presupuestarias. [↑](#footnote-ref-2)
2. Compendio oficial de contribuciones nacionales voluntarias sobre el tema de la aplicación del derecho internacional a la utilización de las tecnologías de la información y las comunicaciones por los Estados, presentado por expertos gubernamentales participantes en el Grupo de Expertos Gubernamentales sobre la promoción de un comportamiento estatal responsable en el ciberespacio en el contexto de la seguridad internacional establecido en virtud de la resolución 73/26 de la Asamblea General \_ [A-76-136-EN.pdf (un-arm.org)](https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf) [↑](#footnote-ref-3)