CENTRO DE ESTUDIOS INTERNACIONALES
GILBERTO BOSQUES

Reunión virtual

6 DE DICIEMBRE DE 2022

Reunión virtual con la Presidencia 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

Inter-Parlamentary Union
For democracy. For everyone

SERIE
UIP
N°15

CENTRO DE ESTUDIOS INTERNACIONALES
GILBERTO BOSQUES
DIPLOMACIA PARLAMENTARIA

Reunión virtual con la Presidencia 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

Creando un ciberespacio seguro para la democracia

6 de diciembre de 2022

Unión Interparlamentaria
Por la democracia. Para todos.

Serie: Unión Interparlamentaria

N° 15

Reunión virtual con la Presidencia 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

Creando un ciberespacio seguro para la democracia

6 de diciembre de 2022

ÍNDICE

I. Nota Conceptual

Unión Interparlamentaria
Por la democracia. Para todos.

Creando un ciberespacio seguro para la democracia
Aportación parlamentaria a las negociaciones para el Convenio de las Naciones Unidas sobre la Ciberdelincuencia con el fin de garantizar el cumplimiento de las necesidades de los ciudadanos y de los parlamentos y sus miembros

Reunión virtual con la Presidencia 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

6 de diciembre de 2022
Sesión 1: programada para la región de Asia y el Pacífico, de 7:00 h a 9:00 h CET
Sesión 2: programada para África, Europa y las Américas, de 16:30 h a 18:30 h CET

Las sociedades han crecido y se han desarrollado en torno a las tecnologías digitales hasta el punto de que todos los aspectos de la sociedad, las infraestructuras críticas —tales como la electricidad, el agua, el gas, las comunicaciones bancarias, el transporte y los hospitales—, dependen de ellas y de internet para proporcionar bienes y servicios con eficiencia. Los usuarios pueden desempeñar sus tareas cotidianas con mucha más eficiencia si las realizan en línea. El ciberespacio se ha ampliado más allá de un reino meramente “técnico” hasta convertirse en una nueva dimensión en la que las actividades e interacciones virtuales reemplazan a las interacciones materiales y físicas. La dependencia de la tecnología digital viene acompañada del riesgo de la ciberdelincuencia contra la sociedad y los individuos, lo que se ha puesto de manifiesto especialmente tras la reciente pandemia de COVID-19 durante la que los ciberataques contra los individuos aumentaron drásticamente.

Los parlamentarios, en calidad de representantes del pueblo, se encuentran en la primera línea de respuesta en materia de ciberdelincuencia. Sus funciones legislativa, supervisora, presupuestaria y representativa son fundamentales para entender y abordar las amenazas actuales a nivel nacional e internacional. Los propios parlamentos no son inmunes a los ciberataques, como puede constatarse en numerosos informes sobre piratería informática, ataques a infraestructuras de comunicaciones y ataques dirigidos a parlamentarios. Estos ciberataques

amenazan con alterar el funcionamiento de las instituciones democráticas, las cuales deben considerarse infraestructura crítica.

Los periodos de sesiones virtuales son una oportunidad exclusiva de informar a la Presidencia del Comité Especial encargada de realizar las negociaciones para un convenio sobre la ciberdelincuencia acerca de las necesidades y la importancia de la participación de los parlamentos y los parlamentarios en el intento mundial por abordar los riesgos cibernéticos de una manera que se encuentre en consonancia con los derechos individuales y las libertades personales. Las sesiones se basarán en las experiencias parlamentarias sobre la exposición a la ciberdelincuencia, su mitigación y la lucha por contrarrestarla, además de postular recomendaciones concretas que resalten el potencial de los parlamentos como centros de coordinación de cara a moldear e implementar un ciberespacio seguro para todos.

Objetivos del evento

1. Concienciar sobre los riesgos y las consecuencias de la ciberdelincuencia en la ciudadanía y las infraestructuras críticas.
2. Compartir “buenas prácticas parlamentarias” y políticas efectivas para abordar la ciberdelincuencia.
3. Identificar y comunicar las disposiciones en relación con la protección de la ciudadanía en la dimensión cibernética y la clasificación de los parlamentos como infraestructura crítica, que los parlamentarios desearían ver incluidas en el convenio.

Este evento se celebrará en línea, en dos sesiones para adecuarse a los participantes, que se encuentran en distintos husos horarios, y propiciar que se escuche el máximo de puntos de vista y se intercambien experiencias. La sesión 1 tendrá lugar únicamente en inglés. La sesión 2 se llevará a cabo en inglés, francés, español y árabe, con interpretación simultánea.

Inscripción

Sesión 1: programada para la región de Asia y el Pacífico, 7:00 h CET (únicamente en inglés)
https://us06web.zoom.us/webinar/register/WN_dMEN_hv2QGO5vUyrHFry0g

Sesión 2: programada para Europa, África y las Américas, 16:30 h CET (en inglés, francés, español y árabe)
https://us06web.zoom.us/webinar/register/WN_HYpQIlTqR_uSqLUt0Zj9tg

II. Perfiles de los Oradores Principales

PERFILES

Honorable Sra. Arda Gerkens

Vicepresidenta del Senado de los Países Bajos

La Señora Gerkens es miembro del Senado de los Países Bajos desde mayo de 2013 y participa en los siguientes consejos y delegaciones interparlamentarias:

- Asuntos Económicos y Clima / Agricultura, Naturaleza y Calidad Alimentaria
- Relaciones del Reino
- Salud Pública, Bienestar y Deporte
- Grupo Neerlandés en la Unión Interparlamentaria
- Delegación Neerlandesa de la Asamblea Interparlamentaria del Benelux
- Consejo Interparlamentario de la Unión de la Lengua Neerlandesa.

Fue miembro de la Cámara de Representantes (*Tweede Kamer*) del 2002 al 2010.

Desde 2015, ha sido Directora General de la Agencia de Expertos en Abuso Infantil en Línea (línea de ayuda neerlandesa).

Su Excelencia Sra. Embajadora Faouzia Mebarki

Presidenta del Consejo de una Convención sobre el Delito Cibernético

Tiene un Diploma de la Escuela Nacional de Administración de Argelia (Sección Diplomática) y un Diploma del Instituto de Estudios Diplomáticos Pedro Gual en Caracas, Venezuela.

En mayo de 2021, fue electa presidenta del Consejo Intergubernamental de composición abierta para elaborar una convención internacional integral sobre la lucha contra el uso de las tecnologías de la información y las comunicaciones con fines delictivos.

Diplomática de carrera, sus asignaciones incluyen cargos como Embajadora en Austria y Eslovaquia y Representante Permanente ante las Organizaciones Internacionales en Viena (desde 2016 hasta la actualidad); Jefa del Gabinete del Ministro de Asuntos de Magreb, Unión Africana y Liga de los

	Estados Árabes (2015); Directora de Países de Europa Central y del Este (2014); Responsable de las relaciones con el Parlamento Europeo en la Embajada de Argelia en Bruselas (2010); Representante ante la UNESCO y responsable de la sección multilateral de la Embajada de Argelia en Roma.
	**Embajadora Brigitte Brenner** **Observadora Permanente de la UIP ante la ONU** Se ha desempeñado como Observadora Permanente de la UIP ante la ONU y otras Organizaciones Internacionales en Viena desde hace casi dos años. Fungió como directora de la UE y Servicios Internacionales en el Parlamento de Austria durante más de diez años. A lo largo de su carrera, ocupó numerosos puestos de alto rango en Austria. Entre otras cosas, se desempeñó como asesora adjunta de política exterior del presidente federal Heinz Fischer y fue coordinadora de gestión de crisis en la Oficina del Canciller de Austria. Ha estado activa en diferentes ONG en el campo del empoderamiento de la mujer y la asistencia para el desarrollo. Tiene un doctorado en Ciencias Políticas por la Universidad de Viena. Estudió Historia y Filología Alemana en la Universidad de Graz y completó su educación de posgrado en la Academia Diplomática de Viena.
	**Sr. Martin Chungong** **Secretario General de la UIP** Se convirtió en el primer africano y el primer no europeo en ser elegido Secretario General de la UIP en 2014 y fue electo para un tercer mandato en julio de 2022. Tiene más de cuatro décadas de experiencia y conocimiento de los parlamentos a nivel nacional e internacional. Ha dedicado su vida profesional a promover y construir la democracia en todo el mundo y es reconocido como líder en el campo del desarrollo de

	programas para ayudar a los parlamentos a convertirse en instituciones democráticas más efectivas, mientras contribuye a la creación de puntos de referencia de gobernanza para fortalecer la democracia. También es miembro de una serie de organismos internacionales que llevan la voz de la comunidad parlamentaria a los foros de igualdad de género, salud, nutrición y Objetivos de Desarrollo Sostenible (ODS), entre otras áreas.

III. Documentos de Apoyo

Naciones Unidas A/AC.291/2

Asamblea General

Distr. general
15 de junio de 2020
Español
Original: inglés

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

Propuesta de esbozo y modalidades de las actividades ulteriores 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

Documento de antecedentes preparado por la Secretaría

I. Introducción

1. En su resolución 74/247, de 27 de diciembre de 2019, titulada “Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos”, la Asamblea General decidió establecer un comité intergubernamental especial de expertos de composición abierta, representativo de todas las regiones, a fin de elaborar una convención internacional integral sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, teniendo plenamente en cuenta los instrumentos internacionales y las iniciativas existentes en los planos nacional, regional e internacional para combatir la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, en particular, la labor y los resultados del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético, de carácter intergubernamental y de composición abierta.

2. En esa misma resolución, la Asamblea General decidió también que el Comité Especial celebrara un período de sesiones de organización de tres días de duración en agosto de 2020 en Nueva York, a fin de acordar el esbozo y las modalidades de sus actividades ulteriores, que se presentarían a la Asamblea General en su septuagésimo quinto período de sesiones para su examen y aprobación.

3. La secretaría preparó el presente documento de antecedentes con arreglo a los mandatos conferidos al Comité Especial en virtud de la resolución 74/247, con miras a facilitar las deliberaciones que mantendrá en su período de sesiones de organización en torno a la estructura de su labor futura encaminada a cumplir su mandato. En el documento se proponen los elementos que conformarán el esbozo de las actividades ulteriores del Comité Especial y se describe en términos generales cómo se organizará el proceso de elaboración de la convención[1].

4. Al preparar el presente documento de antecedentes, la secretaría tuvo en cuenta los siguientes factores:

a) la experiencia relativa a la organización de los procesos de negociación de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y sus Protocolos[2] y de la Convención de las Naciones Unidas contra la Corrupción[3];

b) la organización del plan de trabajo plurianual del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético;

c) la disponibilidad de recursos de gestión de conferencias en los años venideros, que era también un factor importante al proponer la estructura de las actividades ulteriores del Comité Especial.

II. Propuesta de esbozo de las actividades ulteriores del Comité Especial

5. De conformidad con la resolución 74/247, el Comité Especial tiene encomendada la elaboración de una convención internacional integral sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos. Para cumplir su mandato, el Comité podría estudiar la posibilidad de celebrar ocho períodos de sesiones en Viena, entre agosto de 2021 y finales de junio de 2024, a fin de elaborar y aprobar la convención, que se sometería, por conducto de un proyecto de resolución, a la Asamblea General para su examen y aprobación en su septuagésimo noveno período de sesiones, que tendrá lugar en 2024.

6. Con arreglo a la resolución 74/247, durante el proceso de negociación, el Comité Especial tendrá plenamente en cuenta los instrumentos internacionales y las iniciativas existentes en los planos nacional, regional e internacional para combatir

[1] Habida cuenta de que el Comité Especial es un órgano subsidiario de la Asamblea General, se aplicará el Reglamento de la Asamblea General.
[2] Los documentos de los períodos de sesiones del Comité Especial encargado de Elaborar una Convención contra la Delincuencia Organizada Transnacional pueden consultarse en el sitio web www.unodc.org/unodc/en/treaties/CTOC/background/adhoc-committee.html.
[3] Los documentos de los períodos de sesiones del Comité Especial encargado de Negociar una Convención contra la Corrupción pueden consultarse en el sitio web www.unodc.org/unodc/en/treaties/CAC/background/adhoc-committee.html.

la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, en particular, la labor y los resultados del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético, de carácter intergubernamental y de composición abierta. A tal efecto, la secretaría preparará, a petición del Comité, un documento de antecedentes sobre los instrumentos jurídicos internacionales, las recomendaciones y demás documentos existentes en los que se trate la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, con vistas a facilitar el proceso de elaboración de la convención.

III. Propuesta de modalidades de las actividades ulteriores del Comité Especial

7. En esta sección se proponen algunos de los elementos que conformarán la estructura de las actividades ulteriores del Comité Especial, como un calendario viable y flexible de carácter indicativo con los períodos de sesiones del Comité, que se celebrarían en Viena en 2021, 2022, 2023 y 2024.

8. En el cuadro siguiente se propone el calendario provisional de los períodos de sesiones del Comité Especial que se celebrarían en 2021, 2022, 2023 y 2024, así como las tareas que se llevarían a cabo en ellos[4]:

[4] El calendario provisional propuesto se preparó a partir del asesoramiento del Servicio de Gestión de Conferencias de la Oficina de las Naciones Unidas en Viena en lo referente a los recursos disponibles para reuniones, la viabilidad de que se celebren las reuniones y los intervalos en los que es viable que tengan lugar las reuniones habida cuenta de los requisitos en materia de preparación, edición y traducción de los documentos parlamentarios.

Período de sesiones	*Fechas*	*Tareas*
2021		
Primer período de sesiones	2 a 13 de agosto	Examinar y acordar las cuestiones relacionadas con el esbozo y la estructura de la convención
2022		
Segundo período de sesiones	Una semana, entre el 21 de febrero y el 4 de marzo	Examinar y acordar el texto del borrador preliminar de la convención sobre la base de las propuestas y las contribuciones presentadas por los Estados Miembros tras el primer período de sesiones del Comité. El texto sentará las bases de los trabajos ulteriores que el Comité emprenderá en los períodos de sesiones subsiguientes
Tercer período de sesiones	22 de agosto a 2 de septiembre	Seguir profundizando en el texto del proyecto de convención como parte de un planteamiento gradual
Cuarto período de sesiones	12 a 23 de diciembre	Seguir profundizando en el texto del proyecto de convención como parte de un planteamiento gradual
2023		
Quinto período de sesiones	Dos semanas en abril*	Seguir profundizando en el texto del proyecto de convención como parte de un planteamiento gradual
Sexto período de sesiones	Dos semanas de finales de agosto a principios de septiembre	Seguir profundizando en el texto del proyecto de convención. En esta etapa, el Comité podría estudiar la posibilidad de solicitar a todos los grupos regionales que nombren a sus representantes en un grupo al cual se encomendará en el séptimo período de sesiones del Comité que vele por la coherencia del texto en todos los idiomas oficiales de las Naciones Unidas
Séptimo período de sesiones	Dos semanas en diciembre	Seguir profundizando en el texto del proyecto de convención como parte de un planteamiento gradual
2024		
Octavo período de sesiones	Dos semanas antes de finales de junio	Finalizar y aprobar el proyecto de texto de la convención y examinar y aprobar un proyecto de resolución, en cuyo anexo figurará el texto del proyecto de convención y que se someterá a la Asamblea General para su examen y aprobación en su septuagésimo noveno período de sesiones, que tendrá lugar en 2024

* Habida cuenta de su procedimiento de trabajo, el Servicio de Gestión de Conferencias de la Oficina de las Naciones Unidas en Viena no está en condiciones de especificar las fechas de los períodos de sesiones que tendrían lugar en 2023 y 2024. La secretaría mantendrá consultas sobre las fechas provisionales y se informará oportunamente a los Estados Miembros.

9. Si se lo encomienda el Comité, para su primer período de sesiones, la secretaría preparará, partiendo de las propuestas y contribuciones recibidas de los Estados Miembros, un documento de antecedentes consolidado en el que se esbozará la convención y se definirá su estructura. Para el segundo período de sesiones, la secretaría consolidará, a partir de las propuestas y contribuciones formuladas por los Estados Miembros, un borrador preliminar de la convención que se someterá al examen y aprobación del Comité a fin de que este pueda seguir trabajando sobre la base de ese documento. Para cada uno de los períodos de sesiones, la secretaría preparará una versión revisada del proyecto de convención a partir de las propuestas y contribuciones presentadas por los Estados Miembros y del resultado del período de sesiones precedente. La recopilación de las propuestas y contribuciones recibidas de los Estados Miembros antes de cada período de sesiones no privará a las delegaciones de su derecho a presentar las propuestas que estimen apropiadas y oportunas durante el proceso de negociación para que el Comité las examine y adopte una decisión al respecto.

10. De conformidad con el artículo 103 del Reglamento de la Asamblea General, el Comité elegirá su mesa, integrada por 1 Presidente, 13 Vicepresidentes y 1 Relator, teniendo en cuenta una distribución geográfica equitativa, así como la experiencia y la competencia personal de los candidatos. En consonancia con la práctica seguida al elaborar la Convención contra la Delincuencia Organizada y la Convención contra la Corrupción, el Comité podría estudiar la posibilidad de mantener la mesa elegida en el período de sesiones de organización para que siguiera desempeñándose en los períodos de sesiones posteriores, hasta que finalizara y aprobara el proyecto de convención y lo sometiera a la Asamblea General para su examen y aprobación en su septuagésimo noveno período de sesiones, que tendrá lugar en 2024.

11. Además de reunirse en los períodos de sesiones oficiales del Comité Especial, los Estados Miembros podrían reunirse y mantener consultas oficiosamente siguiendo las directrices marcadas por la mesa del Comité como parte de sus esfuerzos para lograr un consenso en cuestiones relacionadas con la elaboración de la convención. Debería considerarse de gran importancia que se garantizaran tanto la transparencia del proceso de negociación como la máxima participación de los Estados.

12. Durante la elaboración de la convención, el Comité Especial podría plantearse si invita a los Estados Miembros a contemplar la posibilidad de organizar una conferencia política de alto nivel para la firma de la convención.

13. El Comité Especial tal vez desee instar a los Estados Miembros a participar plenamente en la elaboración de la convención y a esforzarse por garantizar su representación en todo momento. En ese sentido, el Comité podría estudiar la

posibilidad de reiterar la invitación dirigida a los países donantes en la resolución 74/247 a fin de que presten asistencia a las Naciones Unidas para asegurar la participación activa de los países en desarrollo en la labor del Comité, incluso sufragando los gastos de viaje y alojamiento.

14. Durante el proceso de elaboración, el Comité Especial podría contemplar la posibilidad de tener en cuenta las contribuciones de las organizaciones intergubernamentales, las organizaciones no gubernamentales, la sociedad civil y el sector privado, de conformidad con el Reglamento de la Asamblea General y siguiendo la práctica establecida por el Comité Especial encargado de Elaborar una Convención contra la Delincuencia Organizada Transnacional y el Comité Especial encargado de Negociar una Convención contra la Corrupción[5].

15. El Comité también podría considerar la posibilidad de reiterar la solicitud formulada en la resolución 74/247 para que el Secretario General asigne los recursos necesarios a fin de organizar y apoyar la labor del Comité con cargo al presupuesto por programas de las Naciones Unidas.

16. El Comité Especial podría estudiar la idea de presentar informes sobre la marcha de su labor a la Asamblea General en sus períodos de sesiones septuagésimo sexto, septuagésimo séptimo, septuagésimo octavo y septuagésimo noveno, que se celebrarán en 2021, 2022, 2023 y 2024, respectivamente.

[5] La práctica correspondiente del Comité Especial encargado de Negociar una Convención contra la Corrupción figura en los párrafos 23 a 27 de su informe sobre la labor de sus períodos de sesiones primero a séptimo (A/58/422).

RESOLUCIÓN 74/247: "LUCHA CONTRA LA UTILIZACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES CON FINES DELICTIVOS"

Nota Informativa[6]

Antecedentes

La ciberdelincuencia representa una amenaza en constante evolución para la seguridad de las sociedades, las empresas y los gobiernos. Por su naturaleza se puede considerar un peligro global y sin fronteras por lo que debe ser abordado mediante la cooperación internacional.

En 2001, por primera vez, los países de la Unión Europea reconocieron esta problemática mediante la firma el Convenio de Budapest, constituyéndose como el primer tratado internacional en esta materia. En él se definen los delitos relacionados, además de ser una hoja de ruta para la investigación y el combate de este tipo de delincuencia[7].

Por su parte, el 21 de diciembre de 2010, la Asamblea General de las Naciones Unidas adoptó la Resolución 65/230, mediante la cual solicitó a la Comisión de Prevención del Delito y Justicia Penal (CPDJP) que se creara un grupo intergubernamental de expertos de composición abierta a fin de que realizara un estudio a profundidad acerca de los delitos cibernéticos. Este primer grupo de trabajo no llegó a un consenso sobre la necesidad de un nuevo tratado internacional sobre ciberdelincuencia[8].

Sin embargo, algunos Estados miembros de las Naciones Unidas continuaron trabajando para lograr un tratado. En respuesta a estos esfuerzos la Asamblea General de las Naciones Unidas adoptó la Resolución 73/187, de 17 de diciembre de 2018, sobre la lucha contra la utilización de las tecnologías de la información y la comunicación con fines delictivos[9].

Resolución 74/247

Debido a los intensos trabajos realizados por los algunos países, la Asamblea General de las Naciones Unidas reconoció de manera aún más contundente el

---

[6] Elaborada en el Centro de Estudios Internacionales Gilberto Bosques del Senado mexicano con información citada.

[7] Comisión Europea, *Recomendación de Decisión Del Consejo por la que se autorizan las negociaciones de un convenio internacional integral sobre la lucha contra la utilización de las tecnologías de la información y la comunicación con fines delictivo.* Consultada el 2 de diciembre de 2022 en la URL: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52022PC0132&from=EN

[8] *Ibidem*

[9] *Ibidem*

potencial que representan las tecnologías de la información y las comunicaciones para desarrollar nuevas oportunidades para los criminales y su contribución al aumento de la delincuencia y de la complejidad de los delitos.

Asimismo, la Asamblea manifestó su preocupación por el mal uso que se le puede dar a las llamadas tecnologías emergentes, como la inteligencia artificial, pero reconoció las posibilidades que ofrecen para prevenir y combatir el uso de las tecnologías de la información y las comunicaciones con fines delictivos y manifestaron que la ciberdelincuencia representa un peligro no solo para las personas, sino también para la estabilidad de la infraestructura esencial de los Estados y las empresas. Además de servir para crear nuevas formas de realizar delitos persistentes tales como la trata de personas[10].

Por lo anterior, el 27 de diciembre de 2019, de nueva cuenta la Asamblea General de las Naciones Unidas adoptó una segunda Resolución, la 74/247, sobre el mismo tema, por la cual estableció un comité intergubernamental de expertos ad hoc para crear un convenio internacional integral acerca de la lucha contra la utilización de las tecnologías de la información y la comunicación con fines delictivos[11].

La Resolución especifica que el comité ad hoc debe tomar en cuenta los instrumentos y esfuerzos internacionales existentes a escala nacional, regional e internacional en la lucha contra la utilización de las tecnologías de la información y la comunicación con fines delictivos, en particular el trabajo y los resultados del grupo intergubernamental de expertos[12].

Posteriormente, en mayo de 2021, mediante la Resolución 75/282 se determinaron las modalidades de las negociaciones estableciendo entre otras cosas, que el comité ad hoc debía convocar al menos seis sesiones, de diez días cada una, empezando en enero de 2022, y una sesión de clausura para presentar un proyecto de Convenio a la Asamblea General de las Naciones Unidas en su septuagésimo octavo período de sesiones en 2024[13].

---

[10] Comisión Nacional de Derechos Humanos, *El uso de las nuevas tecnologías y los derechos humanos.* Consultado el 2 de diciembre de 2022 en la URL: https://cdhcm.org.mx/wp-content/uploads/2016/09/dfensor_06_2016.pdf

[11] Asamblea General de Naciones Unidas, *Propuesta de esbozo y modalidades de las actividades ulteriores 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.* Consultado el 2 de diciembre de 2022 en la URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Background_paper/A_AC.291_2_S.pdf

[12] *Ibidem*

[13] *Ibidem*

El 20 de enero de 2022, la Asamblea General decidió aplazar la primera sesión a una fecha posterior debido a la situación de la pandemia de COVID-19 en Nueva York[14].

[14] *Ibidem*

CIBERSEGURIDAD Y CIBERDELINCUENCIA

Nota Informativa[15]

Resumen

En este texto se abordan algunas definiciones relacionadas con la ciberseguridad y la ciberdelincuencia, así como la importancia de la protección de datos personales de la población y los gubernamentales para proteger la estabilidad del Estado. Posteriormente, se exponen las principales amenazas dentro del espacio cibernético, las acciones que se han llevado a cabo internacional y regionalmente y, por último, se presenta la situación actual de México, y algunos cambios previstos para la legislación nacional.

Introducción

La ciberseguridad es definida como las medidas para defender y proteger computadoras, servidores, sistemas electrónicos, redes y usuarios que operen en Internet, así como los datos que se manejan en ellos, de sistemas de ataques maliciosos que puedan comprometer su privacidad o vulneren los sistemas electrónicos de alguna persona, organización, empresa, institución o Estado[16].

Los ataques cibernéticos se dirigen principalmente a corporaciones, ciudadanos individuales y Estados; comúnmente, involucran delitos informáticos como el robo de identidad, el fraude, extorsiones, manipulación de datos o sabotaje informático, aunque con el paso del tiempo, se ha visto que éstos pueden utilizarse de maneras mucho más dañinas en ataques a infraestructuras estratégicas o gubernamentales.

Con el avance de la tecnología, la ciberseguridad se ha convertido en una prioridad para todos los gobiernos del mundo, ya que se protegen los archivos disponibles a través de Internet y por medio de servidores privados, los cuales pueden ser intervenidos para obtener la información que yace dentro. Si un grupo de *hackers* logra obtener información sensible y clasificada sobre el Estado, pueden ocasionar un daño considerable y desestabilizar al país o a una región entera[17].

La ciberseguridad se ha convertido en una necesidad para todas las naciones y todas las personas, debido a la creciente importancia que han adquirido los contenidos electrónicos, así como la necesidad de mantenerlos privados, lo que

[15] Elaborada en el Centro de Estudios Internacionales Gilberto Bosques del Senado mexicano con información citada.
[16] Kaspersky. ¿Qué es la ciberseguridad? Consultado el 20 de octubre de 2022, en: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security
[17] Senado de la República. Gaceta: LXV/2PPO-20/129409. Consultado el 20 de octubre de 2022, en: https://www.senado.gob.mx/64/gaceta_del_senado/documento/129409

genera la necesidad de una mayor inversión para lograr una protección de calidad y continua.

Amenazas

Con las innovaciones tecnológicas han surgido nuevos desafíos para proteger los datos personales, empresariales o gubernamentales. A continuación, se darán definiciones sobre algunos tipos de afectaciones cibernéticas. Por un lado, el *ransomware*, es un tipo de *software* malicioso diseñado para exigir dinero mediante el bloqueo del acceso a los archivos y al sistema informativo hasta que se paga el rescate. Otro es el conocido como el *malware*, que es un tipo de software diseñado para obtener acceso no autorizado o causar daño a una computadora, y la ingeniería social es una táctica usada para engañar a fin de que se revele la información confidencial y esto puede ser a cambio de un pago monetario o de obtener acceso a la información confidencial.

Otro tipo de tácticas para infiltrarse en los dispositivos requeridos es a través del *phishing*, el cual se basa en engañar a los usuarios de Internet para que den sus datos personales o el *hacking*, el cual se describe como un acceso ilegal a la computadora de alguien de manera remota[18].

Uno de los principales problemas en la actualidad es la suplantación de identidad, que es una práctica de envío de correos electrónicos fraudulentos que se asemejan a correos electrónicos oficiales, con el propósito de filtrar correos maliciosos que afectan la imagen o el prestigio de un organismo, institución o de una persona.

Dentro de la Agenda de Ciberseguridad Global, desarrollada por la Unión Internacional de Telecomunicaciones (UIT), se consideran que existen cinco pilares esenciales para la protección de datos[19]:

1. Medidas legales: Incluye una legislación penal sobre delitos cibernéticos, así como un derecho sustantivo, procesal y un reglamento de seguridad cibernética.
2. Medidas técnicas: Incorpora equipos de respuesta a incidentes cibernéticos (CIRT) nacionales y gubernamentales, y establece estándares para organizaciones.

[18] Naciones Unidas. Delito Cibernético. Consultado el 20 de octubre de 2022, en: https://www.un.org/es/events/crimecongress2015/cibercrime.shtml

[19] Oficina de las Naciones Unidas contra la Droga y el Delito. Seguridad cibernética y prevención del Delito Cibernético: Estrategias, Políticas y Programas. Consultado el 20 de octubre de 2022, en: https://www.unodc.org/e4j/es/cybercrime/module-8/key-issues/international-cooperation-on-cybersecurity-matters.html#:~:text=La%20Agenda%20Global%20sobre%20Seguridad%20Cibern%C3%A9tica%20identifica%20cinco%20pilares%20estrat%C3%A9gicos,(consulte%20la%20imagen%203).

3. Estructuras Organizacionales: Establece estrategias para lograr organismos responsables, así como métricas para contar con ciberseguridad.
4. Creación de capacidades: Creación de conciencia pública, además de programas nacionales de educación, programas de investigación y desarrollo y mecanismos de incentivos.
5. Cooperación: Lograr una cooperación interestatal eficiente, concretar acuerdos multilaterales y llevar a cabo foros internacionales.

Debido a que este tipo de delitos muchas veces se cometen de manera transfronteriza, la cooperación entre países es indispensable, ya que puede afectar gravemente la dinámica internacional, incluyendo desde las rutas comerciales hasta las centrales eléctricas[20]. El Gerente de Instituciones del Banco Interamericano de Desarrollo (BID), Moisés J. Schwartz, dio a conocer que "el crimen en línea ya supone, aproximadamente, la mitad de todos los delitos contra la propiedad que tienen lugar en el mundo".

El aumento de la ciberdelincuencia tiene que ver con el crecimiento exponencial del Internet y la tecnología informática, además del hecho de que la gran mayoría de los movimientos de capitales se realizan a través de medios electrónicos, lo que genera más vulnerabilidades y riesgos[21]. De acuerdo con la compañía Cisco, "los ciberdelitos crecen año con año a medida que las personas intentan beneficiarse de los sistemas comerciales vulnerables. A menudo, los atacantes buscan rescates, lo que resulta en que el 53 % de los ciberataques den como resultado daños por USD 500 mil o más"[22].

Situación en América Latina

El aumento de la popularidad del Internet y las redes sociales han hecho que la población se enfrente a amenazas mayores que comprometen su seguridad, que se expongan a ser estafados o a ser intervenidos digitalmente por *hackers,* con el objetivo de robar información o contraseñas para extorsionar o vender esta información a terceros. Ocurre una situación similar con las instancias gubernamentales de todo el mundo, en caso de ser intervenidos, los *hackers* tienen el potencial de sacar a la luz documentos privados de instituciones y de afectar la seguridad nacional.

Internacionalmente, el Convenio de Budapest sobre Delito Cibernético establece lineamientos para combatir algunas infracciones cibernéticas, tales como el derecho

[20] Senado de la República. Op. Cit.
[21] INTERPOL. *Estrategia Mundial contra la Ciberdelincuencia*. Consultado el 4 de diciembre de 2018 en la URL: file:///D:/Respaldo/Senado/Descargas/007-04_Summary_CYBER_Strategy_2017_01_SP%20LR.pdf
[22] Cisco. ¿Cuáles son los ciberataques más comunes? Consultado el 20 de octubre de 2022, en: https://www.cisco.com/c/es_mx/products/security/common-cyberattacks.html

de autor, fraude, pornografía infantil, delitos de odio y violaciones de seguridad dentro de las redes. Igualmente, busca homogeneizar definiciones sobre ciberdelito e intercambiar información sobre la ciberdelincuencia, todo esto con un enfoque basado en los derechos humanos, la libertad de expresión y la libertad de buscar, obtener y comunicar información e ideas de toda índole[23].

"La Organización de Estados Americanos (OEA) ha estado comprometida con temas de seguridad y delincuencia cibernética, fomentando y apoyando la labor de los Estados Miembro para fortalecer su capacidad de proteger a las personas, las economías y la infraestructura crítica en esta materia". Uno de los proyectos desarrollados por la OEA es su Programa de Seguridad Cibernética del Comité Interamericano contra el Terrorismo, el cual se encarga de elaborar estrategias de seguridad cibernética nacionales, facilitar los ejercicios de gestión de crisis con operadores de la industria nacional crítica, así como crear conciencia sobre las amenazas y oportunidades relacionadas con la seguridad cibernética en la región[24].

Cada uno de los Estados adecua sus estrategias y sus legislaciones dependiendo de los riesgos y amenazas concretas que identifican y enfrentan, así como los recursos disponibles para combatirlos. El informe Ciberseguridad 2016, publicado por la OEA y el BID, indica que cualquier estrategia nacional debe de tener algunos elementos generales, dentro de los cuales se encuentra la existencia de un órgano coordinador que se encargue de la supervisión y coordinación de las gestiones de entidades y la resolución de disputas, igualmente, se requiere de una asignación de responsabilidades para la seguridad cibernética entre las dependencias de gobierno, especialmente para los sectores de energía, telecomunicaciones y finanzas[25].

Dos ejemplos en la región sobre esta materia son Argentina y Brasil.

En Argentina, en 2015, se estableció una Oficina Nacional bajo la dirección de la Secretaría de Protección de Infraestructuras Críticas de Información y Ciberseguridad, la cual se centra en desarrollar normas y estándares de seguridad cibernéticas, por lo cual se han tipificado nuevos delitos, entre los que se encuentran cometer fraude informático, causar daño informático y propagar virus, acceder

[23] OEA. Convenio sobre la ciberdelincuencia. 2001. Consultado el 21 de octubre de 2022, en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf
[24] Ciberseguridad. Latinoamérica. Consultado el 21 de octubre de 2022, en: https://ciberseguridad.com/normativa/latinoamerica/#Argentina
[25] Banco Interamericano de Desarrollo. Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe? 2016. Consultado el 24 de octubre de 2022, en: https://publications.iadb.org/publications/spanish/document/Ciberseguridad-%C2%BFEstamos-preparados-en-Am%C3%A9rica-Latina-y-el-Caribe.pdf

ilícitamente a sistemas informáticos y causar daño informático o sabotaje informático, solo por mencionar algunos[26].

En Brasil se han desarrollado más de mil proyectos de ley relacionados con Internet y cuenta con un marco civil conocido como la Declaración de Derechos, el cual establece principios fundamentales para Internet como la protección de la privacidad, la libertad de expresión y la neutralidad de la red. Igualmente, Brasil cuenta con una Ley General de Protección de Datos personales de 2018, y la Guía de Referencias para la Protección de Infraestructuras Críticas de Información, la cual fue la base para la creación de un comando dentro de las fuerzas armadas destinado a la defensa cibernética formal. Por otro lado, se les ha otorgado a algunas instituciones públicas como a la Agencia Nacional de Telecomunicaciones (ANATEL), la Secretaría Nacional de Protección al Consumidor (SENACON) y el Consejo Administrativo de Defensa Económica (CADE), la capacidad de proteger legalmente los datos de la población y el Estado[27].

Situación actual en México

El panorama de la ciberseguridad en México es complejo, ya que, a inicios de octubre de 2022, un grupo de *hackers* se infiltró en la Secretaría de la Defensa Nacional y accedieron a información que data del año 2016 hasta septiembre de 2022. El total de información excedió los seis terabytes, lo que equivale a miles de archivos, correos electrónicos, cartas, videos y textos clasificados[28].

Tras el hackeo sufrido, se vio la urgencia de legislar sobre ciberseguridad y el robustecimiento de los sistemas informáticos del Estado, ya que varias instituciones del país son constantemente atacadas a través de este tipo de medios. El senador Ricardo Monreal, presidente de la Junta de Coordinación Política del Senado, señaló que es necesario retomar el tema de la ciberseguridad dentro del Congreso para entregar una legislación que otorgue certidumbre en casos como los que sufrió la SEDENA.

México es el sexto país más vulnerable del mundo a ataques de *malware*, pero también es reconocido como uno de los países mejor preparados en el continente para hacerle frente a este tipo de amenazas, esto según el Índice Global de Seguridad (IGC) de la UIT. Dentro del reporte, el país tiene un índice de 81.68 puntos, por encima de la media, y la calificación lo coloca en la clasificación 52 de 194 naciones. Continentalmente, los países mejor posicionados en materia de seguridad, de acuerdo con el índice de la UIT, son: Estados Unidos (100); Canadá

[26] Ciberseguridad. Argentina. Consultado el 21 de octubre de 2022, en: https://ciberseguridad.com/normativa/latinoamerica/argentina/
[27] Ciberseguridad. Brasil. Consultado el 21 de octubre de 2022, en: https://ciberseguridad.com/normativa/latinoamerica/brasil/
[28] Capital 21. Reportan hackeo a SEDENA por el grupo internacional denominado “Guacamaya”.

(97.67); Brasil (96.6); México (81.68); Uruguay (75.15); y República Dominicana (75.07)[29].

Por otro lado, "El Índice de Riesgo de Ciberataques Financieros, que es estimado con base en una metodología del Fondo Monetario Internacional (FMI), mide el riesgo cibernético en el sector para distintos países, con base en noticias de periódicos internacionales. Así, Banxico precisó que, al aplicar la metodología del FMI con noticias de enero de 2017 a marzo de 2022, México está en la posición 39 de 105 países con una calificación de 3.68 por ciento"[30].

La ciberdelincuencia ha estado en aumento en los últimos años; entre más usuarios haya en las redes sociales y dentro de Internet, habrá más posibilidades de que sean víctimas de *hackers*, estafadores o extorsionadores, por lo cual se hace extremadamente importante crear conciencia sobre los peligros dentro del mundo digital y hacer recomendaciones sobre qué acciones tomar cuando se reciben mensajes o links de personas desconocidas. Desde 2021 se han presentado más de 25 mil denuncias relacionadas con ciberataques y ciberdelitos.

Por otro lado, del total de fraudes cibernéticos al segundo semestre de 2021, de acuerdo con las reclamaciones iniciadas por Condusef, poco más de 2.5 millones estuvieron relacionadas con el comercio por Internet; 119 mil 179 por banca móvil; 89 mil 324 corresponden a operaciones por Internet de personas físicas; 3 mil 076 operaciones por Internet de personas morales; y 29 pagos por celular[31].

Para la Cámara de Comercio Estadounidense en México, los principales desafíos para el país en el tema de ciberseguridad son[32]:

- Exceso de información no deseada (20.5 millones).
- Mensajes de personas desconocidas (16.4 millones).
- Infección por virus (10.6 millones).
- Fraudes con información financiera personal (3.2 millones).
- Violación a la privacidad (2.5 millones).

Con el objetivo de combatir la ciberdelincuencia, se han planteado algunas modificaciones y actualizaciones al marco legislativo de México. El país no cuenta

[29] El Heraldo de México. México destaca en ciberseguridad: Banxico. 20 de junio de 2022. Consultado el 21 de octubre de 2022, en: https://heraldodemexico.com.mx/economia/2022/6/20/mexico-destaca-en-ciberseguridad-banxico-414994.html
[30] Ídem.
[31] Senado de la República. Op. Cit.
[32] Ídem.

con una ley dedicada específicamente al delito cibernético, sin embargo, el artículo 211 del Código Penal prevé el delito informático[33].

A lo largo de la LXIV Legislatura se presentaron, tanto en el Senado de la República como en la Cámara de Diputados, 11 iniciativas, de las cuales 10 están pendientes de discusión en las comisiones de sus cámaras de origen y la faltante se encuentra en las comisiones de la Cámara revisora. Cuatro de las iniciativas ajustan el Código Penal Federal, cuatro implican la promulgación de una nueva ley y tres son propuestas de reforma a la Ley de Seguridad Nacional[34].

El 27 de septiembre de 2022, el presidente de la Cámara de Senadores, Alejandro Armenta Mier, presentó una iniciativa que tiene el objetivo de atender la ciberdelincuencia, además de incluir la cobertura en materia de conectividad e implica una ampliación en derechos dentro del ciberespacio. La iniciativa plantea modificar el Código Penal, así como definir la ciberseguridad como la práctica de proteger sistemas, redes y aplicaciones, así como dispositivos y programas de ataques digitales, los cuales generalmente se hacen con el fin de acceder, modificar o destruir información confidencial. Como parte de la misma iniciativa, se tiene en consideración una pena de dos a seis años de prisión y una multa de 100 a 500 días de salario[35].

El pasado 6 de octubre, miembros de la Cámara de Senadores instalaron una mesa permanente en materia de ciberseguridad para robustecer al Estado mexicano contra futuros hackeos.

[33] Senado de la República. Op. Cit.
[34] Ídem.
[35] Senado de la República. Versión estenográfica de la conferencia de prensa del senador Alejandro Armenta Mier, presidente de la Mesa Directiva del Senado de la República. 17 de octubre de 2022. Consultado el 21 de octubre de 2022, en: https://comunicacionsocial.senado.gob.mx/informacion/prensa/3968-version-estenografica-de-la-conferencia-de-prensa-del-senador-alejandro-armenta-mier-presidente-de-la-mesa-directiva-del-senado-de-la-republica

CENTRO DE ESTUDIOS INTERNACIONALES
GILBERTO BOSQUES
DIPLOMACIA PARLAMENTARIA

Coordinadora General
Aliza Klip Moshinsky

Directora General
María Rosa López González

Colaboraron en la elaboración de este documento:
Miguel Venegas Ramírez
Alejandro Osornio Ramos