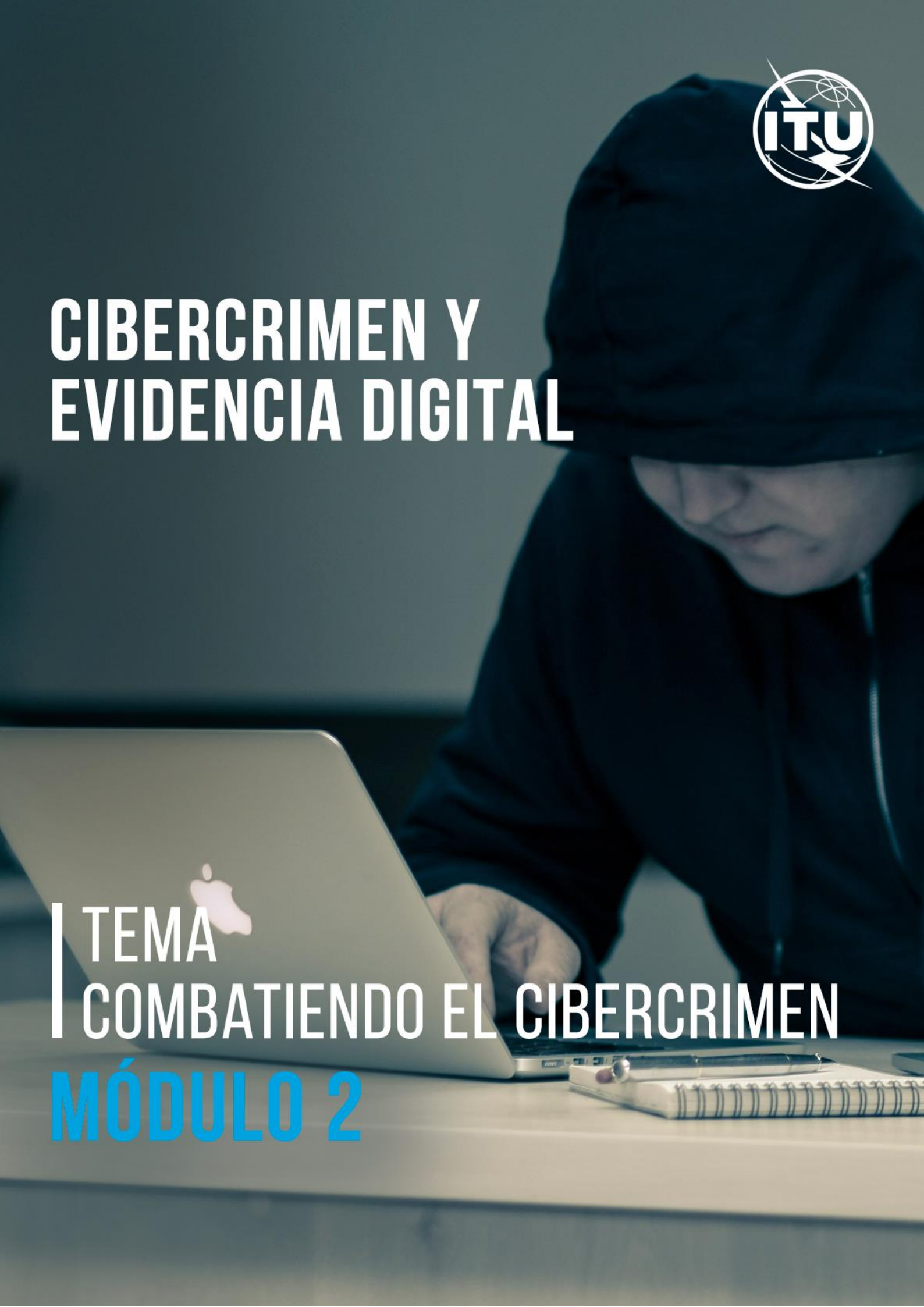


CIBERCRIMEN Y EVIDENCIA DIGITAL

TEMA
COMBATIENDO EL CIBERCRIMEN

MÓDULO 2

TABLA DE CONTENIDOS

MÓDULO 2

En el presente módulo se contempla una breve introducción a los aspectos básicos de respuesta al cibercrimen.

COMBATIENDO EL CIBERCRIMEN

El Objetivo del módulo es aprender y aplicar los conceptos básicos y la importancia de la lucha contra el cibercrimen.

1. MARCO LEGAL Y RESPUESTA INTERNACIONAL

Junto con el desarrollo y utilización de las TIC, no solo se han incrementado los ciberdelitos y métodos delictivos, sino también han surgido nuevas formas de investigar los ciberdelitos, logrando ampliar en gran medida las capacidades de las entidades encargadas de hacer cumplir la ley. Esto lleva a que los delincuentes utilicen también nuevas herramientas para impedir su identificación y obstaculizar las investigaciones, lo cual representa un desafío para el combate de los ciberdelitos.

Los países buscan contar con un marco legal adecuado para investigar y procesar los ciberdelitos. Sin embargo, la aparición de nuevas formas de ciberdelito requiere un proceso de ajuste constante del marco legal, de las leyes penales nacionales y la redacción de nueva legislación.

Otro de los puntos a tomar en cuenta es que el ciberespacio no tiene fronteras, y los usuarios conectados a internet pueden interactuar libremente con recursos u otras personas conectadas y ubicadas en cualquier lugar del mundo. Entonces, si se comete un ciberdelito necesitamos realizar una investigación que involucra a varios países. Incluso, si todos los implicados se ubican en un solo país y se utilizó el internet para realizar un delito, hay probabilidad de que las pruebas de la comisión del delito se encuentren fuera del país. En efecto, la mayoría de transacciones electrónicas se hacen mediante procesos de transferencia de datos que transitan por más de un país. La conectividad y el Internet conducen el tráfico a través de rutas o encaminamientos temporales y posiblemente distintos. Por ejemplo, cuando contratamos un espacio en la nube para contar con un servidor web, los delincuentes y sus objetivos se encuentran situados en países distintos; y los investigadores de esos ciberdelitos deben cooperar con las entidades encargadas de hacer cumplir la ley de todos los países involucrados. Dado que, por motivos de soberanía nacional, no se permite realizar investigaciones en

el territorio de los países interesados, sin el permiso de las autoridades nacionales, los investigadores de ciberdelitos necesitan el apoyo y la participación de los gobiernos de los países involucrados.

Resulta difícil llevar a cabo la cooperación en materia de ciberdelito aplicando los principios tradicionales de asistencia mutua jurídica. El carácter oficial de los requisitos jurídicos y el tiempo necesario para colaborar con las entidades extranjeras encargadas de hacer cumplir la ley suelen obstaculizar las investigaciones, que las más de las veces se realizan en periodos muy breves. Ahora bien, algunos datos que resultan indispensables para detectar delitos suelen borrarse rápidamente. El hecho de que el periodo de investigación sea corto resulta problemático, ya que toma tiempo organizar un marco de asistencia mutua dentro de los regímenes jurídicos tradicionales. El principio de doble criminalidad también plantea dificultades, cuando el acto considerado no se tipifica como delito en uno de los países que participan en la investigación. Además, es posible que los delincuentes incluyan deliberadamente a terceros países en sus ataques para obstaculizar las investigaciones.

Cabe la posibilidad de que los delincuentes seleccionen deliberadamente objetivos situados fuera de su propio país y actúen a partir de países con una legislación de lucha contra el ciberdelito inadecuada. La armonización de las leyes sobre el ciberdelito y de la cooperación internacional contribuiría positivamente en este contexto. Uno de los instrumentos más conocidos de cooperación internacional es el Convenio del Consejo de Europa sobre la Ciberdelincuencia (Convenio de Budapest).

2. CONVENIO SOBRE LA CIBERDELINCUENCIA DE BUDAPEST

El Convenio sobre la Ciberdelincuencia (Convention on Cybercrime), conocido como Convenio de Budapest (COE, Serie Tratados Europeos N° 185), fue suscrito en dicha ciudad el 23 de noviembre de 2001 en el marco de los Estados miembros del Consejo de Europa, y se encuentra en vigor a partir del 1 de julio de 2004.

El Convenio de Budapest, según establece su Preámbulo tiene por fin “incrementar la eficacia de las investigaciones y procedimientos penales relativos a los delitos relacionados con sistemas y datos informáticos, así como permitir la obtención de pruebas electrónicas de los delitos” (Consejo de Europa, Preámbulo), mediante “una cooperación internacional reforzada, rápida y eficaz en materia penal”.

El Convenio de Budapest tiene por objeto promover la armonización de la legislación que regula el cibercrimen, a nivel del derecho penal sustantivo de cada Estado Parte; mejorar las capacidades nacionales para la investigación de este tipo de delitos, conforme al derecho procesal de cada país; y establecer un régimen ágil y efectivo de cooperación internacional principalmente para facilitar la investigación transnacional de estos delitos.

En el anexo se presenta el texto completo del Convenio de Budapest para mayor detalle.

3. ACTIVIDADES DE LA UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

La Unión Internacional de Telecomunicaciones (UIT) tiene en su agenda la temática de ciberseguridad y desde hace mucho tiempo realiza actividades para apoyar las iniciativas, principalmente, de los países en desarrollo. Sus actividades son múltiples, sin embargo, en el presente texto solamente abordaremos algunas de ellas, dejando las demás para ser tratadas durante el desarrollo del curso.

Actualmente, a través del Sector de Desarrollo, mantiene el “programa de ciberseguridad” ofreciendo a los miembros de la UIT, en particular a los países en desarrollo, la oportunidad y las herramientas para aumentar las capacidades de ciberseguridad a nivel nacional, con el fin de mejorar la seguridad, generar confianza y confianza en el uso de las TIC, haciendo que el ámbito digital sea más seguro para todos. La labor y el mandato del programa de ciberseguridad se basan en el Objetivo 2 del Plan de Acción de Buenos Aires adoptado en la Conferencia Mundial de Desarrollo de las Telecomunicaciones de 2017 y las resoluciones relacionadas que se mencionan a continuación:

Conferencia de Plenipotenciarios de la UIT (PP):

- Resolución 130 (Rev. Dubai 2018) "El fortalecimiento del papel de la UIT en la construcción de confianza y seguridad en la utilización de tecnologías de la información y de la comunicación".
- Resolución 174 (Busan 2014) "El papel de la UIT con respecto a las cuestiones de política pública internacional relacionadas con el riesgo de uso ilícito de las tecnologías de la información y las comunicaciones".
- Resolución 179 (Rev. Dubai 2018) "El papel de la UIT en la protección de la infancia en línea".

Conferencia Mundial de Desarrollo de las Telecomunicaciones de la UIT (CMDT):

- Resolución 45 (Dubai 2014) "Mecanismos para mejorar la cooperación en materia de ciberseguridad, incluida la respuesta y lucha contra el spam".
- Resolución 67 (Buenos Aires 2017) "El papel del Sector de Desarrollo de las Telecomunicaciones de la UIT en la protección infantil en línea".
- Resolución 69 (Buenos Aires 2017) "Facilitación de la creación de equipos nacionales de respuesta a incidentes informáticos, especialmente para países en desarrollo, y cooperación entre ellos".

Asamblea Mundial de Normalización de las Telecomunicaciones de la UIT (WTSA):

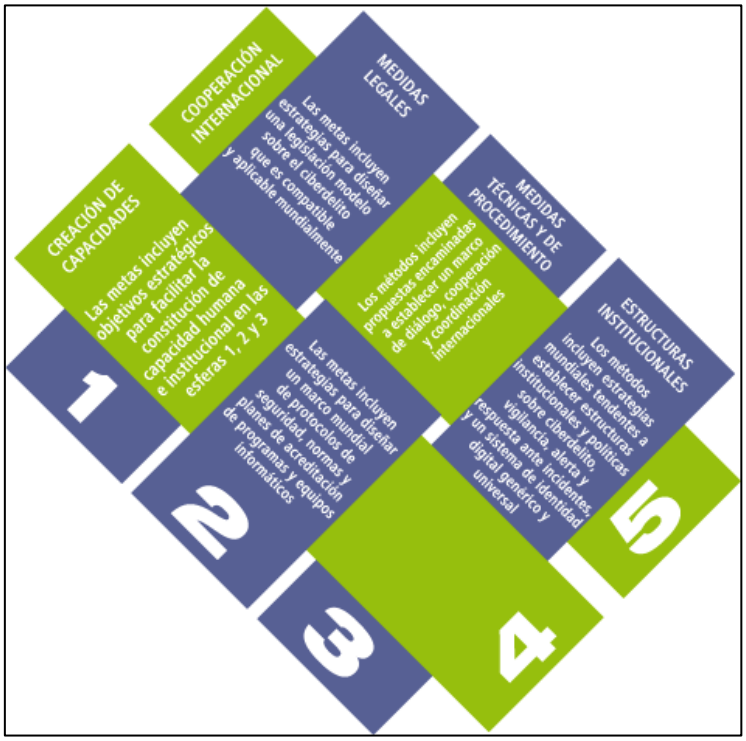
- Resolución 50 (Hammamet 2016) "Ciberseguridad".
- Resolución 52 (Hammamet 2016) "Lucha contra el correo no deseado"
- Resolución 58 (Dubai 2012) "Fomentar la creación de equipos nacionales de respuesta a incidentes informáticos, especialmente para los países en desarrollo".

La agenda de ciberseguridad global

Como resultado de la Conferencia Mundial de la Sociedad de la Información, la UIT fue designada como único facilitador de la Línea de Acción C5 consagrada a la creación de confianza y seguridad en la utilización de las TIC. En la segunda reunión de facilitación relativa a la Línea de Acción C5 convocada en 2007, el Secretario General de la UIT destacó la importancia de la cooperación internacional en la lucha contra el ciberdelito y anunció el lanzamiento de una Agenda sobre Ciberseguridad Global de la UIT. La Agenda se centra en siete objetivos clave, basados a su vez en cinco pilares estratégicos, entre otros la elaboración de estrategias para la formulación de legislación modelo sobre el ciberdelito. Los siete objetivos son los siguientes:

1. Preparar estrategias que promuevan el desarrollo de una legislación modelo sobre ciberdelito, que resulte aplicable a escala mundial y sea compatible con las medidas legislativas ya adoptadas en los diferentes países y regiones.
2. Definir estrategias mundiales para crear las adecuadas estructuras institucionales nacionales y regionales, así como definir las correspondientes políticas para luchar contra el ciberdelito.
3. Diseñar una estrategia que permita establecer un conjunto mínimo y mundialmente aceptado de criterios de seguridad y planes de acreditación para equipos, aplicaciones y sistemas informáticos.
4. Definir estrategias para crear un marco mundial con miras a vigilar, alertar y responder ante incidentes y garantizar así la coordinación transfronteriza en lo que concierne a las iniciativas nuevas y existentes.

5. Diseñar estrategias mundiales tendentes a crear y apoyar un sistema de identidad digital genérico y universal y las correspondientes estructuras institucionales para garantizar el reconocimiento internacional de credenciales digitales.
6. Concebir una estrategia global para facilitar la creación de capacidad humana institucional con el fin de promover los conocimientos técnicos y prácticos en todos los sectores y las esferas antes mencionadas.
7. Formular propuestas para establecer un marco conducente a una estrategia mundial multipartita que fomente la cooperación, el diálogo y la coordinación internacionales en todas las esferas precitadas.



Pilares estratégicos de La Agenda sobre Ciberseguridad Global de la UIT

La Agenda sobre Ciberseguridad Global tuvo su sede en la Asociación Internacional Multilateral contra el ciberterrorismo – IMPACT (International Multilateral Partnership Against Cyber-Terrorism), que fue creada el 20 de mayo de 2008 en la Cumbre Mundial sobre Ciberseguridad (WCSS) en Kuala Lumpur (Malasia); y aunque todas las actividades de la asociación de la UIT con IMPACT finalizaron en el 2016, la Agenda sobre Ciberseguridad Global de la UIT se encuentra vigente.

La Conferencia de Plenipotenciarios de la UIT de 2018, celebrada en Dubái, adoptó la Resolución 130: Fortalecimiento del papel de la UIT en la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación. La

Resolución resuelve, entre otras cosas se utilice el marco de la Agenda sobre Ciberseguridad Global (ACG) para seguir encauzando la labor de la Unión, que en sus esfuerzos por crear confianza y seguridad en la utilización de las tecnologías de la información y la comunicación (TIC).

En el año 2020 se ha elaborado el Proyecto de Directrices para la utilización de la Agenda de ciberseguridad global y será aprobado este año 2021.

Índice de ciberseguridad global

El Índice Global de Ciberseguridad (GCI) es una referencia confiable que **mide el compromiso de los países con la ciberseguridad a nivel global**, para generar conciencia sobre la importancia y las diferentes dimensiones del tema. Dado que la ciberseguridad tiene un amplio campo de aplicación, que abarca muchas industrias y varios sectores, el nivel de desarrollo o participación de cada país se evalúa a lo largo de cinco pilares: (i) Medidas legales, (ii) Medidas técnicas, (iii) Medidas organizativas, (iv) Desarrollo de capacidades, y (v) Cooperación, y luego se agregan en una puntuación general. El modelo toma en cuenta 20 indicadores:

MEDIDAS LEGALES (Jurídicas)
1. Legislación sustantiva en materia de ciberdelincuencia 1.1. Legislación sustantiva sobre comportamientos ilegales en línea (sobre acceso ilegal, injerencia ilegal, intercepción de dispositivos, sistemas informáticos y datos realizando el ingreso, alteración o supresión de datos; y robo de datos e identidad) 1.2. Disposiciones sobre falsificación informática (piratería/violación de derechos de autor) 1.3. Legislación sustantiva sobre seguridad en línea (contra los delitos relacionados con el material racista y xenófobo en línea; contra el acoso en línea y el abuso contra la dignidad/integridad personal; y legislación relativa a la protección de menores en Internet)
2. Regulación de la ciberseguridad: leyes y reglamentos sobre ciberseguridad 2.1. Protección de datos personales/privacidad 2.2. Notificación de infracciones/incidentes de datos 2.3. Requisitos para auditorías de ciberseguridad 2.4. Aplicación de normas de ciberseguridad reconocidas a nivel internacional dentro del sector público (agencias gubernamentales), e integrados en la infraestructura crítica (incluso si los ejecuta el sector privado). Estas normas incluyen, entre otras, las elaboradas por las agencias siguientes: ISO, UIT, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, CEI, NERC, NIST, FIPS, PCI DSS, etc
MEDIDAS TÉCNICAS
3. Existencia de CERT/CIRT/CSIRT nacionales / gubernamentales 3.1. Sensibilización en materia de ciberseguridad 3.2. Ejercicios de ciberseguridad, como cibersimulacros 3.3. Publicación de información sobre ciberamenazas inminentes y sobre el comportamiento recomendado 3.4. Participación en el Foro sobre los equipos de seguridad y respuesta ante incidentes. www.first.org

3.5. Afiliaciones a otras comunidades CERT/CIRT/CSIRT 3.6. CertificaciónTF-CSIRT-SIM3
4. Existencia de CERT/CIRT/CSIRT Sectoriales 4.1. Actividades de sensibilización para un sector 4.2. Cibersimulacros nacionales 4.3. Publicación de información sobre ciberamenazas e incidentes acaecidos en el sector
5. Marco nacional para la aplicación de las normas de ciberseguridad 5.1. Marco para la aplicación/adopción de las normas de ciberseguridad 5.2. Marco normas internacionales o de otro tipo conexas (UIT-T, ISO/CEI, NIST, ANSI/ISA, etc.)
6. Protección de la Infancia en Línea (mecanismos o capacidades de comunicación para proteger a la infancia en línea)
MEDIDAS ORGANIZATIVAS
7. Estrategia nacional de ciberseguridad 7.1. Estrategia/política nacional de ciberseguridad 7.2. Plan de acción/hoja de ruta definido para la implementación de la gobernanza de ciberseguridad 7.3. Estrategia nacional de Protección de la Infancia en Línea
8. Existencia de una Agencia nacional responsable de la ciberseguridad a nivel nacional 8.1. Coordinación de la ciberseguridad a nivel nacional 8.2. La capacitación en materia de ciberseguridad nacional 8.3. Las iniciativas de Protección de la Infancia en Línea a nivel nacional
9. Medición de la ciberseguridad 9.1. Auditorías de ciberseguridad a nivel nacional 9.2. sistema de medición para la evaluación de los riesgos del ciberespacio a nivel nacional 9.3. Mediciones para evaluar el nivel de desarrollo de la ciberseguridad a nivel nacional
CREACIÓN DE CAPACIDADES (Capacitación)
10. Campañas públicas sobre ciberseguridad 10.1. campañas de sensibilización públicas específicas para sectores como las PYME, las empresas privadas y las agencias estatales 10.2. campañas de sensibilización públicas para la sociedad civil 10.3. campañas de sensibilización públicas para la población en general 10.4. campañas de sensibilización públicas para los ancianos 10.5. campañas de sensibilización públicas para las personas con necesidades especiales 10.6. campañas de sensibilización públicas para padres, docentes y niños
11. Formación para profesionales de la ciberseguridad 11.1. Cursos de formación profesional en ciberseguridad preparados o apoyados por el Gobierno para el fomento de la formación de la mano de obra (técnica, ciencias sociales, etc.) en ciberseguridad y fomento de la certificación de profesionales del sector público o privado. 11.2. Existe un programa de acreditación para profesionales de la ciberseguridad (institutos de acreditación de profesionales de la ciberseguridad) 11.3. Programas/formaciones/cursos sectoriales nacionales para profesionales de la ciberseguridad (fuerzas del orden, personal judicial y jurídico, pymes, funcionarios públicos y miembros de Gobierno)
12. Programas educativos o programas de estudios sobre ciberseguridad (primaria, secundaria, superior)
13. Programas de investigación y desarrollo en ciberseguridad 13.1. Programas de I+D en ciberseguridad del sector privado 13.2. programas de I+D en ciberseguridad del sector público

13.3. Participación de las instituciones de enseñanza superior, como instituciones académicas y universidades, en las actividades de I+D
14. Industria nacional de la ciberseguridad
15. Mecanismos estatales de incentivos para fomentar la ciberseguridad: 15.1. Fomentar la capacitación en ciberseguridad 15.2. Fomentar el desarrollo de la industria de ciberseguridad.
MEDIDAS DE COOPERACIÓN
16. Acuerdos bilaterales de cooperación en materia de ciberseguridad con otros países 16.1. Acuerdos de compartición de información 16.2. Acuerdos de capacitación 16.3. Acuerdos de asistencia jurídica mutua
17. Participación del gobierno en mecanismos internacionales relacionados con la ciberseguridad
18. Acuerdos multilaterales en materia de ciberseguridad 18.1. Acuerdo multilaterales sobre cooperación en materia de ciberseguridad 18.2. Acuerdo de compartición de información 18.3. Acuerdos de capacitación
19. Acuerdos con el sector privado (con empresas locales y empresas extranjeras domiciliadas en el país)
20. Acuerdos entre agencias (entre distintos órganos estatales en materia de ciberseguridad)

Indicadores del marco de referencia para el Global Cybersecurity Index
Fuente: Unión Internacional de Telecomunicaciones

Guía para desarrollar una estrategia nacional de ciberseguridad - Compromiso estratégico en ciberseguridad

Mejorar la ciberseguridad y proteger las infraestructuras de información críticas es esencial para la seguridad y el bienestar económico de todas las naciones, particularmente en el movimiento global hacia la economía digital y la sociedad de la información.

A nivel nacional, la ciberseguridad es una responsabilidad compartida que requiere una acción coordinada de prevención, preparación, respuesta y recuperación de incidentes por parte de las autoridades gubernamentales, el sector privado y la sociedad civil. Para que esto funcione sin problemas y para garantizar un ámbito digital seguro, protegido y resistente, es necesario un marco o estrategia integral que debe desarrollarse, implementarse y ejecutarse en un enfoque de múltiples partes interesadas. Este marco a menudo se conoce como Estrategia Nacional de Ciberseguridad y es un elemento crítico para la seguridad socioeconómica de cualquier país.

Por ello, la UIT brinda entrenamiento en línea gratuito sobre el Ciclo de vida, principios y buenas prácticas de desarrollo e implementación de estrategias nacionales de ciberseguridad; y además ha publicado una guía de referencia para ayudar a los países a crear un marco nacional de ciberseguridad eficaz.

El objetivo de la guía es promover el pensamiento estratégico y ayudar a los líderes nacionales y los responsables de la formulación de políticas a desarrollar, establecer e implementar estrategias nacionales de ciberseguridad en todo el mundo.

Esta guía es un recurso que proporciona un marco que ha sido acordado por organizaciones con experiencia demostrada y diversa en esta esfera temática y que se basa en sus trabajos previos en este campo, ofreciendo la visión general más exhaustiva disponible hasta la fecha de lo que constituyen las estrategias nacionales de ciberseguridad que han tenido éxito. Se presenta un conjunto de buenas prácticas que se agrupan en distintas esferas de interés de una estrategia nacional de ciberseguridad.

5.6 Esfera prioritaria 6 – Legislación y reglamentación

5.6.1 Promulgar legislación sobre ciberdelincuencia

La estrategia debe promover la instauración de un marco jurídico nacional que defina claramente lo que constituye ciberactividad prohibida y que tenga por objeto reducir la delincuencia en línea. En la mayoría de los casos, este marco adopta la forma de legislación sobre la ciberdelincuencia, que se materializa promulgando nuevas leyes específicas o enmendando las existentes (por ejemplo, el código penal, las leyes que regulan la banca, las telecomunicaciones y otros sectores).

La estrategia también debe fomentar la creación de un proceso para supervisar la aplicación y revisión de la legislación y los mecanismos de gobernanza, identificar las lagunas y el traslapo de autoridades, y aclarar y priorizar los ámbitos que requieren modernización (por ejemplo, las leyes existentes, como las antiguas leyes de telecomunicaciones).

5.6.2 Reconocer y salvaguardar los derechos y libertades individuales

La estrategia debe salvaguardar las garantías procesales esenciales (en el caso de investigaciones y enjuiciamientos penales), así como los derechos de protección de datos, incluida la protección de la privacidad de los datos personales (posiblemente mediante el desarrollo de un marco de protección de datos y de la privacidad) y de libertad de expresión, con arreglo al principio de los derechos humanos fundamentales.

5.6.3 Crear mecanismos de observancia

La estrategia debe promover el establecimiento de mecanismos nacionales de observancia (tanto de aplicación como de incentivos). Estos mecanismos deben establecerse para prevenir, combatir y mitigar las acciones dirigidas contra la confidencialidad, la integridad y la disponibilidad de los sistemas e infraestructuras de TIC, así como las amenazas contra los datos informáticos, de conformidad con el marco jurídico antes mencionado. Deben abarcar, entre otras cosas, las particularidades de la investigación digital, la interceptación lícita de las comunicaciones y la utilización de pruebas electrónicas.

5.6.4 Promover la capacitación para la observancia de la ley

La estrategia debe alentar la capacitación para la observancia de la legislación sobre ciberdelincuencia, incluida la capacitación y formación de las diversas partes implicadas en la lucha contra la ciberdelincuencia (por ejemplo, jueces, fiscales, abogados, fuerzas de seguridad, especialistas forenses y otros investigadores). Las fuerzas de seguridad deberían recibir formación especializada para interpretar y aplicar las leyes nacionales sobre ciberdelincuencia (es decir, traducir la ley en conceptos técnicos y viceversa); detectar, disuadir, investigar y enjuiciar eficazmente los delitos cibernéticos; y colaborar eficazmente con la industria

y los servicios de seguridad internacionales (por ejemplo, INTERPOL, Europol) para contrarrestar la ciberdelincuencia y fomentar la ciberseguridad.

5.6.5 Establecer procesos interinstitucionales

La estrategia debe identificar y reconocer los mandatos de los organismos nacionales con la autoridad principal encargada de la observancia de la legislación en materia de ciberdelincuencia, de los responsables de proteger la infraestructura esencial y de los responsables de garantizar el cumplimiento de todos los requisitos internacionales en

5.6.6 Apoyar la cooperación internacional contra la ciberdelincuencia

La estrategia debe demostrar el compromiso de proteger a la sociedad contra la ciberdelincuencia en todo el mundo, mediante la ratificación, siempre que sea posible y de conformidad con la agenda nacional general, de los acuerdos internacionales sobre ciberdelincuencia o acuerdos equivalentes para contrarrestar el delito cibernético, y mediante la promoción de mecanismos de coordinación para hacer frente a la ciberdelincuencia internacional. A tal efecto, puede ser necesario armonizar la legislación nacional con las obligaciones de los tratados internacionales y los acuerdos bilaterales, por ejemplo, mediante el establecimiento de asistencia judicial recíproca, la autorización de investigaciones y enjuiciamientos transfronterizos, la tramitación de pruebas digitales y la extradición.

4. SITUACIÓN ACTUAL DEL CIBERCRIMEN

Con el incremento del uso de las tecnologías de la información y comunicación y del internet, sobre todo en el último año a raíz de la pandemia provocada por la covid-19, sin duda también se han incrementado los ciberdelitos en todas sus modalidades. Veamos algunas estadísticas al respecto.

- Informe sobre delitos en Internet 2020 (FBI)
  El Centro de Quejas de Delitos en Internet del FBI ha publicado su informe anual. El Informe sobre delitos en Internet de 2020 incluye información de 791,790 quejas de presuntos delitos en Internet, un aumento de más de 300,000 quejas desde 2019, y pérdidas reportadas que superan los $ 4,2 mil millones.

  Los tres principales delitos denunciados por las víctimas en 2020 fueron las estafas de phishing, las estafas de impago / no entrega y la extorsión. Las víctimas perdieron mayor cantidad de dinero debido a estafas por correo electrónico empresarial, esquemas de romance y confianza, y fraude de inversiones. En particular, 2020 vio la aparición de estafas que explotan la pandemia de COVID-19.

2020 CRIME TYPES

By Victim Count

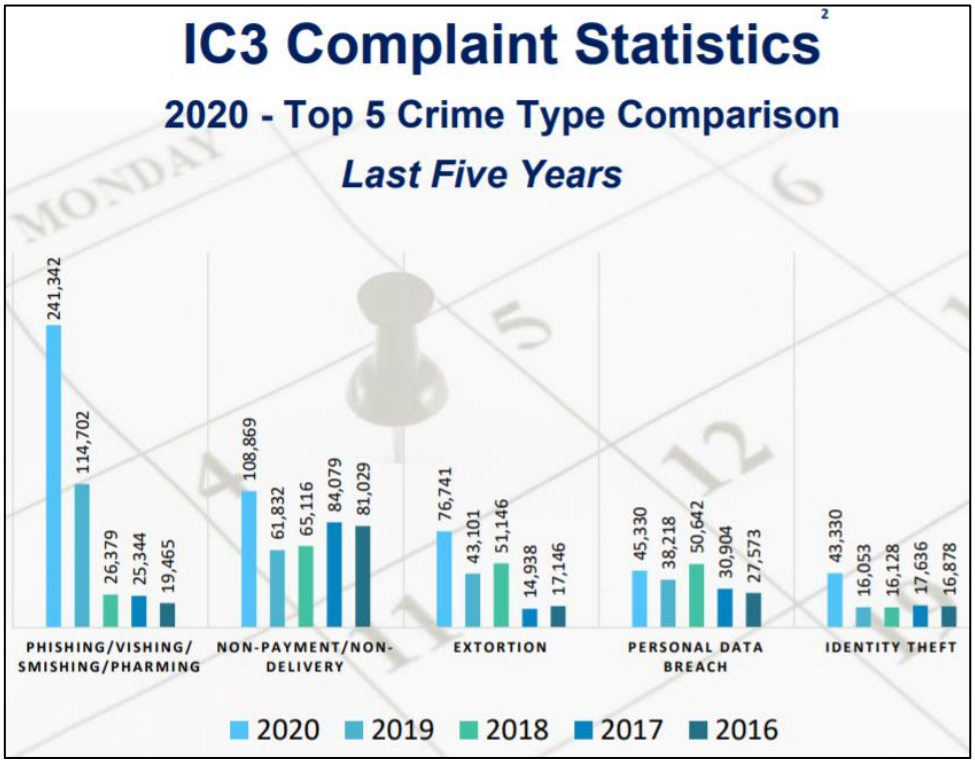
Crime Type	Victims	Crime Type	Victims
Phishing/Vishing/Smishing/Pharming	241,342	Other	10,372
Non-Payment/Non-Delivery	108,869	Investment	8,788
Extortion	76,741	Lottery/Sweepstakes/Inheritance	8,501
Personal Data Breach	45,330	IPR/Copyright and Counterfeit	4,213
Identity Theft	43,330	Crimes Against Children	3,202
Spoofing	28,218	Corporate Data Breach	2,794
Misrepresentation	24,276	Ransomware	2,474
Confidence Fraud/Romance	23,751	Denial of Service/TDoS	2,018
Harassment/Threats of Violence	20,604	Malware/Scareware/Virus	1,423
BEC/EAC	19,369	Health Care Related	1,383
Credit Card Fraud	17,614	Civil Matter	968
Employment	16,879	Re-shipping	883
Tech Support	15,421	Charity	659
Real Estate/Rental	13,638	Gambling	391
Advanced Fee	13,020	Terrorism	65
Government Impersonation	12,827	Hacktivist	52
Overpayment	10,988		

2020 Crime Types *Continued*

By Victim Loss

Crime Type	Loss	Crime Type	Loss
BEC/EAC	$1,866,642,107	Overpayment	$51,039,922
Confidence Fraud/Romance	$600,249,821	Ransomware	**$29,157,405
Investment	$336,469,000	Health Care Related	$29,042,515
Non-Payment/Non-Delivery	$265,011,249	Civil Matter	$24,915,958
Identity Theft	$219,484,699	Misrepresentation	$19,707,242
Spoofing	$216,513,728	Malware/Scareware/Virus	$6,904,054
Real Estate/Rental	$213,196,082	Harassment/Threats Violence	$6,547,449
Personal Data Breach	$194,473,055	IPR/Copyright/Counterfeit	$5,910,617
Tech Support	$146,477,709	Charity	$4,428,766
Credit Card Fraud	$129,820,792	Gambling	$3,961,508
Corporate Data Breach	$128,916,648	Re-shipping	$3,095,265
Government Impersonation	$109,938,030	Crimes Against Children	$660,044
Other	$101,523,082	Denial of Service/TDos	$512,127
Advanced Fee	$83,215,405	Hacktivist	$50
Extortion	$70,935,939	Terrorism	$0
Employment	$62,314,015		
Lottery/Sweepstakes/Inheritance	$61,111,319		
Phishing/Vishing/Smishing/Pharming	$54,241,075		

Fuente: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf



Fuente: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

- Según el "Informe del costo de una violación de datos de 2020", patrocinado por IBM Security y realizado por el Ponemon Institute, las violaciones de datos globales cuestan a las empresas $ 3.86 millones por violación, en promedio. El estudio encuestó a más de 500 organizaciones en todo el mundo entre agosto de 2019 y abril de 2020. Los factores de costo incluidos en la encuesta incluyeron actividades legales, reglamentarias y técnicas relacionadas con las infracciones. La información de identificación personal de los clientes se expuso en el 80 por ciento de las infracciones que ocurrieron el año pasado. Casi el 40 por ciento de los incidentes maliciosos fueron causados por credenciales robadas o comprometidas y configuraciones incorrectas de la nube. Los atacantes utilizaron correos electrónicos y contraseñas previamente expuestos en una de cada cinco infracciones estudiadas, derivadas de más de 8.500 millones de registros expuestos en 2019. Las empresas que experimentaron violaciones de las redes corporativas mediante el uso de credenciales robadas o comprometidas tuvieron casi $ 1 millón agregado a los costos de violación de datos sobre el promedio global, o $ 4.77 millones. Las configuraciones incorrectas de la nube se utilizaron para violar las redes casi el 20 por ciento de las veces, lo que aumentó los costos de la violación en más de medio millón de dólares a $ 4.41 millones en promedio. Los actores de amenazas patrocinados por el estado fueron el tipo de adversario más dañino encontrado en el estudio de 2020, aunque representaron el 13 por ciento de todos los ataques. Los costos de violación resultantes promediaron $ 4.43 millones. La pandemia de COVID-

19 trajo más riesgo de violaciones de datos porque las condiciones de trabajo remoto crearon entornos menos controlados.

- Gartner proyectó que las empresas gastarían más de $ 123 mil millones en seguridad en 2020 y proyectos que calculan crecerán a $ 170,4 mil millones para 2022.
- La pandemia de COVID-19 en curso también ha tenido un impacto importante en la seguridad cibernética. Las estafas en línea aumentaron más del 400% en marzo de 2020 en comparación con los meses anteriores, según el bufete de abogados internacional Reed Smith, mientras que Google reveló que estaba bloqueando más de 18 millones de correos electrónicos de malware y phishing relacionados con COVID-19 todos los días.
- Tamaño de la actividad del delito cibernético

  Las filtraciones de datos dieron como resultado la exposición de 36 mil millones de registros en los primeros tres trimestres de 2020, según una investigación de RiskBased Security. A pesar de esto, el número de infracciones denunciadas públicamente disminuyó en un 51% en comparación con el mismo período del año pasado.

  El uso de malware aumentó en un 358% hasta 2020, y el uso de ransomware aumentó en un 435% en comparación con el año anterior, según un estudio de Deep Instinct. Solo en julio de 2020 se registró un aumento del 653% en la actividad maliciosa en comparación con el mismo mes de 2019.

  Más del 90% de las organizaciones de atención médica sufrieron al menos una brecha de ciberseguridad en los tres años anteriores, según el informe de US Healthcare Cybersecurity Market 2020 .
- Los cibedelitos cuestan a las organizaciones $ 2.9 millones por minuto, y las principales empresas pierden $ 25 por minuto como resultado de las filtraciones de datos, según la investigación de RiskIQ .

  Según una investigación de IBM , se necesitan 280 días para encontrar y contener el ciberataque promedio, mientras que el ataque promedio cuesta $ 3.86 millones.

- Prácticas deficientes de ciberseguridad

  El equipo de Digital Shadows Photon Research descubrió que más de 15 mil millones de credenciales de 100,000 violaciones de datos estaban disponibles en la web oscura, de las cuales 5 mil millones eran únicas. Esto incluyó combinaciones de contraseña y nombre de usuario para servicios de transmisión de música, banca en línea y cuentas de redes sociales.

- Los datos de Cisco estiman que los ataques distribuidos de denegación de servicio (DDoS) crecerán a 15,4 millones en 2023, más del doble de los 7,9 millones de 2018.

- Los ataques DDoS se volvieron más frecuentes en 2020, y el informe NETSCOUT Threat Intelligence registró 4,83 millones de ataques en la primera mitad del año. Eso equivale a 26.000 ataques por día y 18 por minuto.

5. BIBLIOGRAFÍA

Guía de ciberseguridad para los países en desarrollo. Edición 2007, Unión Internacional de Telecomunicaciones

Comprender el delito cibernético: fenómenos, desafíos y respuesta legal, Unión Internacional de Telecomunicaciones, 2014

Guía para desarrollar una estrategia nacional de ciberseguridad: compromiso estratégico en ciberseguridad. Unión Internacional de Telecomunicaciones, 2018

Índice de ciberseguridad global 2020. Unión Internacional de Telecomunicaciones, 2021

https://www.itu.int/en/action/cybersecurity/Pages/gca-guidelines.aspx, agosto 2021

https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics, agosto 2021

6. ANEXO

CONSEJO DE EUROPA
Convenio sobre la ciberdelincuencia

Budapest, 23.XI.2001

PREÁMBULO

Los Estados miembros del Consejo de Europa y los demás Estados signatarios del presente Convenio;

Considerando que el objetivo del Consejo de Europa es conseguir una unión más estrecha entre sus miembros;

Reconociendo el interés de intensificar la cooperación con los Estados Partes en el presente Convenio;

Convencidos de la necesidad de aplicar, con carácter prioritario, una política penal común encaminada a proteger a la sociedad frente a la ciberdelincuencia, entre otras formas, mediante la adopción de la legislación adecuada y el fomento de la cooperación internacional;

Conscientes de los profundos cambios provocados por la digitalización, la convergencia y la globalización continua de las redes informáticas;

Preocupados por el riesgo de que las redes informáticas y la información electrónica sean utilizadas igualmente para cometer delitos y de que las pruebas relativas a dichos delitos sean almacenadas y transmitidas por medio de dichas redes;

Reconociendo la necesidad de una cooperación entre los Estados y el sector privado en la lucha contra la ciberdelincuencia, así como la necesidad de proteger los legítimos intereses en la utilización y el desarrollo de las tecnologías de la información;

En la creencia de que la lucha efectiva contra la ciberdelincuencia requiere una cooperación internacional en materia penal reforzada, rápida y operativa;

Convencidos de que el presente Convenio resulta necesario para prevenir los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, mediante la tipificación de esos actos, tal y como se definen en el presente Convenio, y la asunción de poderes suficientes para luchar de forma efectiva contra dichos delitos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones que permitan una cooperación internacional rápida y fiable;

Conscientes de la necesidad de garantizar el debido equilibrio entre los intereses de la acción penal y el respeto de los derechos humanos fundamentales consagrados en el Convenio de Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) y otros tratados internacionales aplicables en materia de derechos humanos, que reafirman el derecho de todos a defender sus opiniones sin interferencia alguna, así como la libertad de expresión, que comprende la libertad de buscar, obtener y comunicar información e ideas de todo tipo, sin consideración de fronteras, así como el respeto de la intimidad;

Conscientes igualmente del derecho a la protección de los datos personales, tal y como se reconoce, por ejemplo, en el Convenio del Consejo de Europa de 1981 para la protección de las personas con respecto al tratamiento informatizado de datos personales;

Considerando la Convención de las Naciones Unidas sobre los Derechos del Niño (1989) y el Convenio de la Organización Internacional del Trabajo sobre las peores formas de trabajo de los menores (1999);

Teniendo en cuenta los convenios existentes del Consejo de Europa sobre cooperación en materia penal, así como otros tratados similares celebrados entre los Estados miembros del Consejo de Europa y otros Estados, y subrayando que el presente Convenio pretende completar dichos Convenios con objeto de dotar de mayor eficacia las investigaciones y los procedimientos penales relativos a los delitos relacionados con los sistemas y datos informáticos, así como facilitar la obtención de pruebas electrónicas de los delitos;

Congratulándose de las recientes iniciativas encaminadas a mejorar el entendimiento y la cooperación internacional en la lucha contra la ciberdelincuencia, incluidas las medidas adoptadas por las Naciones Unidas, la OCDE, la Unión Europea y el G8;

Recordando las recomendaciones del Comité de Ministros n.º R (85) 10 relativa a la aplicación práctica del Convenio europeo de asistencia judicial en materia penal, en relación con las comisiones rogatorias para la vigilancia de las telecomunicaciones, n.º R (88) 2 sobre medidas encaminadas a luchar contra la piratería en materia de propiedad intelectual y derechos afines, n.º R (87) 15 relativa a la regulación de la utilización de datos personales por la policía, n.º R (95) 4 sobre la protección de los datos personales en el ámbito de los servicios de telecomunicaciones, con especial referencia a los servicios telefónicos, así como n.º R (89) 9 sobre la delincuencia relacionada con la informática, que ofrece directrices a los legisladores nacionales para la definición de determinados delitos informáticos, y n.º R (95) 13 relativa a las cuestiones de procedimiento penal vinculadas a la tecnología de la información;

Teniendo en cuenta la Resolución n.º 1, adoptada por los Ministros europeos de Justicia en su XXI Conferencia (Praga, 10 y 11 de junio de 1997), que recomendaba al Comité de Ministros apoyar las actividades relativas a la ciberdelincuencia desarrolladas por el Comité Europeo de Problemas Penales (CDPC) para aproximar las legislaciones penales nacionales y permitir la utilización de medios de investigación eficaces en materia de delitos informáticos, así como la Resolución n.º 3, adoptada en la XXIII Conferencia de Ministros europeos de Justicia (Londres, 8 y 9 de junio de 2000), que animaba a las Partes negociadoras a proseguir sus esfuerzos para encontrar soluciones que permitan que el mayor número posible de Estados pasen a ser Partes en el Convenio, y reconocía la necesidad de un sistema rápido y eficaz de cooperación internacional que refleje debidamente las exigencias específicas de la lucha contra la ciberdelincuencia;

Teniendo asimismo en cuenta el Plan de Acción adoptado por los Jefes de Estado y de Gobierno del Consejo de Europa con ocasión de su Segunda Cumbre (Estrasburgo, 10 y 11 de octubre de 1997), para buscar respuestas comunes ante el desarrollo de las

nuevas tecnologías de la información, basadas en las normas y los valores del Consejo de Europa,

Han convenido en lo siguiente:

CAPÍTULO I
Terminología

Artículo 1. Definiciones.

A los efectos del presente Convenio:

a) Por «sistema informático» se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa;

b) por «datos informáticos» se entenderá cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función;

c) por «proveedor de servicios» se entenderá:

i) Toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar por medio de un sistema informático, y

ii) cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios de ese servicio;

d) por «datos sobre el tráfico» se entenderá cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente.

CAPÍTULO II
Medidas que deberán adoptarse a nivel nacional

Sección 1. Derecho penal sustantivo

Título 1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

Artículo 2. Acceso ilícito.

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático. Cualquier Parte podrá exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático.

Artículo 3. Interceptación ilícita.

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos. Cualquier Parte podrá exigir que el delito se haya

cometido con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

Artículo 4. Interferencia en los datos.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos.

2. Cualquier Parte podrá reservarse el derecho a exigir que los actos definidos en el apartado 1 provoquen daños graves.

Artículo 5. Interferencia en el sistema.

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos.

Artículo 6. Abuso de los dispositivos.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a) La producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de:

i) Un dispositivo, incluido un programa informático, diseñado o adaptado principalmente para la comisión de cualquiera de los delitos previstos de conformidad con los anteriores artículos 2 a 5;

ii) Una contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático,

con el fin de que sean utilizados para la comisión de cualquiera de los delitos contemplados en los artículos 2 a 5; y

b) la posesión de alguno de los elementos contemplados en los anteriores apartados a.i) o ii) con el fin de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2 a 5. Cualquier Parte podrá exigir en su derecho interno que se posea un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

2. No podrá interpretarse que el presente artículo impone responsabilidad penal en los casos en que la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición mencionadas en el apartado 1 del presente artículo no tengan por objeto la comisión de un delito previsto de conformidad con los artículos 2 a 5 del presente Convenio, como es el caso de las pruebas autorizadas o de la protección de un sistema informático.

3. Cualquier Parte podrá reservarse el derecho a no aplicar lo dispuesto en el apartado 1 del presente artículo, siempre que la reserva no afecte a la venta, la distribución o cualquier otra puesta a disposición de los elementos indicados en el apartado 1.a.ii) del presente artículo.

Título 2. Delitos informáticos

Artículo 7. Falsificación informática.

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno, cuando se cometa de forma deliberada e ilegítima, la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles. Cualquier Parte podrá exigir que exista una intención fraudulenta o una intención delictiva similar para que se considere que existe responsabilidad penal.

Artículo 8. Fraude informático.

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante:

a) Cualquier introducción, alteración, borrado o supresión de datos informáticos;

b) cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona.

Título 3. Delitos relacionados con el contenido

Artículo 9. Delitos relacionados con la pornografía infantil.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a) La producción de pornografía infantil con vistas a su difusión por medio de un sistema informático;

b) la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático;

c) la difusión o transmisión de pornografía infantil por medio de un sistema informático,

d) la adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona;

e) la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.

2. A los efectos del anterior apartado 1, por «pornografía infantil» se entenderá todo material pornográfico que contenga la representación visual de:

a) Un menor comportándose de una forma sexualmente explícita;

b) una persona que parezca un menor comportándose de una forma sexualmente explícita;

c) imágenes realistas que representen a un menor comportándose de una forma sexualmente explícita.

3. A los efectos del anterior apartado 2, por «menor» se entenderá toda persona menor de dieciocho años. No obstante, cualquier Parte podrá establecer un límite de edad inferior, que será como mínimo de dieciséis años.

4. Cualquier Parte podrá reservarse el derecho a no aplicar, en todo o en parte, las letras d) y e) del apartado 1, y las letras b) y c) del apartado 2.

Título 4. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

Artículo 10. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de la propiedad intelectual, según se definan en la legislación de dicha Parte, de conformidad con las obligaciones asumidas en aplicación del Acta de París de 24 de julio de 1971 por la que se revisó el Convenio de Berna para la protección de las obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre la propiedad intelectual, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de los derechos afines definidas en la legislación de dicha Parte, de conformidad con las obligaciones que ésta haya asumido en aplicación de la Convención Internacional sobre la protección de los artistas intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre las obras de los intérpretes y ejecutantes y los fonogramas, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

3. En circunstancias bien delimitadas, cualquier Parte podrá reservarse el derecho a no exigir responsabilidad penal en virtud de los apartados 1 y 2 del presente artículo, siempre que se disponga de otros recursos efectivos y que dicha reserva no vulnere las obligaciones internacionales que incumban a dicha Parte en aplicación de los instrumentos internacionales mencionados en los apartados 1 y 2 del presente artículo.

Título 5. Otras formas de responsabilidad y de sanciones

Artículo 11. Tentativa y complicidad.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno cualquier complicidad intencionada con vistas a la comisión de alguno de los delitos previstos de conformidad con los artículos 2 a 10 del presente Convenio, con la intención de que se cometa ese delito.

2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno cualquier tentativa de comisión de alguno de las delitos previstos de conformidad con los artículos 3 a 5, 7, 8, 9.1.a) y c) del presente Convenio, cuando dicha tentativa sea intencionada.

3. Cualquier Estado podrá reservarse el derecho a no aplicar, en todo o en parte, el apartado 2 del presente artículo.

Artículo 12. Responsabilidad de las personas jurídicas.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que pueda exigirse responsabilidad a las personas jurídicas por los delitos previstos de conformidad con el presente Convenio, cuando sean cometidos por cuenta de las mismas por cualquier persona física, tanto en calidad individual como en su condición de miembro de un órgano de dicha persona jurídica, que ejerza funciones directivas en la misma, en virtud de:

a) Un poder de representación de la persona jurídica;

b) una autorización para tomar decisiones en nombre de la persona jurídica;

c) una autorización para ejercer funciones de control en la persona jurídica.

2. Además de los casos ya previstos en el apartado 1 del presente artículo, cada Parte adoptará las medidas necesarias para asegurar que pueda exigirse responsabilidad a una persona jurídica cuando la falta de vigilancia o de control por parte de una persona física mencionada en el apartado 1 haya hecho posible la comisión de un delito previsto de conformidad con el presente Convenio en beneficio de dicha persona jurídica por una persona física que actúe bajo su autoridad.

3. Con sujeción a los principios jurídicos de cada Parte, la responsabilidad de una persona jurídica podrá ser penal, civil o administrativa.

4. Dicha responsabilidad se entenderá sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido el delito.

Artículo 13. Sanciones y medidas.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que los delitos previstos de conformidad con los artículos 2 a 11 puedan dar lugar a la aplicación de sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad.

2. Cada Parte garantizará la imposición de sanciones o de medidas penales o no penales efectivas, proporcionadas y disuasorias, incluidas sanciones pecuniarias, a las personas jurídicas consideradas responsables de conformidad con el artículo 12.

Sección 2. Derecho procesal

Título 1. Disposiciones comunes

Artículo 14. Ámbito de aplicación de las disposiciones sobre procedimiento.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para establecer los poderes y procedimientos previstos en la presente Sección para los fines de investigaciones o procedimientos penales específicos.

2. Salvo que se establezca específicamente otra cosa en el artículo 21, cada Parte aplicará los poderes y procedimientos mencionados en el apartado 1 del presente artículo a:

a) Los delitos previstos de conformidad con los artículos 2 a 11 del presente Convenio;

b) otros delitos cometidos por medio de un sistema informático; y

c) la obtención de pruebas electrónicas de un delito.

3. a) Cualquier Parte podrá reservarse el derecho a aplicar las medidas indicadas en el artículo 20 exclusivamente a los delitos o categorías de delitos especificados en la reserva, siempre que el ámbito de dichos delitos o categorías de delitos no sea más reducido que el de los delitos a los que esa Parte aplique las medidas indicadas en el artículo 21. Las Partes procurarán limitar dichas reservas para permitir la aplicación más amplia posible de la medida indicada en el artículo 20.

b) Cuando, como consecuencia de las limitaciones existentes en su legislación vigente en el momento de la adopción del presente Convenio, una Parte no pueda aplicar las medidas indicadas en los artículos 20 y 21 a las comunicaciones transmitidas en el sistema informático de un proveedor de servicios:

i) Utilizado en beneficio de un grupo restringido de usuarios, y

ii) que no utilice las redes públicas de comunicaciones ni esté conectado a otro sistema informático, ya sea público o privado,

dicha Parte podrá reservarse el derecho a no aplicar dichas medidas a esas comunicaciones. Cada Parte procurará limitar este tipo de reservas de forma que se permita la aplicación más amplia posible de las medidas indicadas en los artículos 20 y 21.

Artículo 15. Condiciones y salvaguardas.

1. Cada Parte se asegurará de que el establecimiento, la ejecución y la aplicación de los poderes y procedimientos previstos en la presente sección están sujetas a las condiciones y salvaguardas previstas en su derecho interno, que deberá garantizar una protección adecuada de los derechos humanos y de las libertades, incluidos los derechos derivados de las obligaciones asumidas en virtud del Convenio del Consejo de Europa para la protección de los derechos humanos y las libertades fundamentales (1950), del Pacto Internacional de derechos civiles y políticos de las Naciones Unidas (1966), y de otros instrumentos internacionales aplicables en materia de derechos humanos, y que deberá integrar el principio de proporcionalidad.

2. Cuando resulte procedente dada la naturaleza del procedimiento o del poder de que se trate, dichas condiciones incluirán, entre otros aspectos, la supervisión judicial u otra forma de supervisión independiente, los motivos que justifiquen la aplicación, y la limitación del ámbito de aplicación y de la duración del poder o del procedimiento de que se trate.

3. Siempre que sea conforme con el interés público y, en particular, con la correcta administración de la justicia, cada Parte examinará la repercusión de los poderes y procedimientos previstos en la presente sección en los derechos, responsabilidades e intereses legítimos de terceros.

Título 2. Conservación rápida de datos informáticos almacenados

Artículo 16. Conservación rápida de datos informáticos almacenados.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para permitir a sus autoridades competentes ordenar o imponer de otra manera la conservación rápida de determinados datos electrónicos, incluidos los datos sobre el tráfico, almacenados por medio de un sistema informático, en particular cuando existan razones para creer que los datos informáticos resultan especialmente susceptibles de pérdida o de modificación.

2. Cuando una Parte aplique lo dispuesto en el anterior apartado 1 por medio de una orden impartida a una persona para conservar determinados datos almacenados que se encuentren en posesión o bajo el control de dicha persona, la Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a esa persona a conservar y a proteger la integridad de dichos datos durante el tiempo necesario, hasta un máximo de noventa días, de manera que las autoridades competentes puedan conseguir su revelación. Las Partes podrán prever que tales órdenes sean renovables.

3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar al encargado de la custodia de los datos o a otra persona encargada de su conservación a mantener en secreto la aplicación de dichos procedimientos durante el plazo previsto en su derecho interno.

4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Artículo 17. Conservación y revelación parcial rápidas de datos sobre el tráfico.

1. Para garantizar la conservación de los datos sobre el tráfico en aplicación de lo dispuesto en el artículo 16, cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias:

a) Para asegurar la posibilidad de conservar rápidamente dichos datos sobre el tráfico con independencia de que en la transmisión de esa comunicación participaran uno o varios proveedores de servicios, y

b) para garantizar la revelación rápida a la autoridad competente de la Parte, o a una persona designada por dicha autoridad, de un volumen suficiente de datos sobre el tráfico para que dicha Parte pueda identificar a los proveedores de servicio y la vía por la que se transmitió la comunicación.

2. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Título 3. Orden de presentación

Artículo 18. Orden de presentación.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar:

a) A una persona que se encuentre en su territorio que comunique determinados datos informáticos que posea o que se encuentren bajo su control, almacenados en un sistema informático o en un medio de almacenamiento de datos informáticos; y

b) a un proveedor de servicios que ofrezca prestaciones en el territorio de esa Parte que comunique los datos que posea o que se encuentren bajo su control relativos a los abonados en conexión con dichos servicios.

2. Los poderes y procedimientos mencionados en el presente artículo están sujetos a lo dispuesto en los artículos 14 y 14.

3. A los efectos del presente artículo, por «datos relativos a los abonados» se entenderá toda información, en forma de datos informáticos o de cualquier otra forma, que posea un proveedor de servicios y esté relacionada con los abonados a dichos servicios, excluidos los datos sobre el tráfico o sobre el contenido, y que permita determinar:

a) El tipo de servicio de comunicaciones utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio;

b) la identidad, la dirección postal o geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso o información sobre facturación y pago que se encuentre disponible sobre la base de un contrato o de un acuerdo de prestación de servicios;

c) cualquier otra información relativa al lugar en que se encuentren los equipos de comunicaciones, disponible sobre la base de un contrato o de un acuerdo de servicios.

Título 4. Registro y confiscación de datos informáticos almacenados

Artículo 19. Registro y confiscación de datos informáticos almacenados.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a registrar o a tener acceso de una forma similar:

a) A un sistema informático o a una parte del mismo, así como a los datos informáticos almacenados en el mismo; y

b) a un medio de almacenamiento de datos informáticos en el que puedan almacenarse datos informáticos,

en su territorio.

2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para asegurar que, cuando sus autoridades procedan al registro o tengan acceso de una forma similar a un sistema informático específico o a una parte del mismo, de conformidad con lo dispuesto en el apartado 1.a, y tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte del mismo situado en su territorio, y dichos datos sean lícitamente accesibles a través del sistema inicial o estén disponibles para éste, dichas autoridades puedan ampliar rápidamente el registro o la forma de acceso similar al otro sistema.

3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a confiscar o a obtener de una forma similar los datos informáticos a los que se haya tenido acceso en aplicación de lo dispuesto en los apartados 1 ó 2. Estas medidas incluirán las siguientes facultades:

a) Confiscar u obtener de una forma similar un sistema informático o una parte del mismo, o un medio de almacenamiento de datos informáticos;

b) realizar y conservar una copia de dichos datos informáticos;

c) preservar la integridad de los datos informáticos almacenados de que se trate;

d) hacer inaccesibles o suprimir dichos datos informáticos del sistema informático al que se ha tenido acceso.

4. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite toda la información necesaria, dentro de lo razonable, para permitir la aplicación de las medidas indicadas en los apartados 1 y 2.

5. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Título 5. Obtención en tiempo real de datos informáticos

Artículo 20. Obtención en tiempo real de datos sobre el tráfico.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a:

a) Obtener o grabar mediante la aplicación de medios técnicos existentes en su territorio, y

b) obligar a un proveedor de servicios, dentro de los límites de su capacidad técnica:

i) a obtener o grabar mediante la aplicación de medios técnicos existentes en su territorio, o

ii) a prestar a las autoridades competentes su colaboración y su asistencia para obtener o grabar

en tiempo real los datos sobre el tráfico asociados a comunicaciones específicas transmitidas en su territorio por medio de un sistema informático.

2. Cuando una Parte, en virtud de los principios consagrados en su ordenamiento jurídico interno, no pueda adoptar las medidas indicadas en el apartado 1.a), podrá adoptar en su lugar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos sobre el tráfico asociados a determinadas comunicaciones transmitidas en su territorio mediante la aplicación de los medios técnicos existentes en el mismo.

3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se ha ejercido cualquiera de los poderes previstos en el presente artículo, así como toda información al respecto.

4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Artículo 21. Interceptación de datos sobre el contenido.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a las autoridades competentes, por lo que respecta a una serie de delitos graves que deberán definirse en su derecho interno:

a) A obtener o a grabar mediante la aplicación de medios técnicos existentes en su territorio, y

b) a obligar a un proveedor de servicios, dentro de los límites de su capacidad técnica:

i) A obtener o a grabar mediante la aplicación de los medios técnicos existentes en su territorio, o

ii) a prestar a las autoridades competentes su colaboración y su asistencia para obtener o grabar

en tiempo real los datos sobre el contenido de determinadas comunicaciones en su territorio, transmitidas por medio de un sistema informático.

2. Cuando una Parte, en virtud de los principios consagrados en su ordenamiento jurídico interno, no pueda adoptar las medidas indicadas en el apartado 1.a), podrá adoptar en su lugar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos sobre el contenido de determinadas comunicaciones transmitidas en su territorio mediante la aplicación de los medios técnicos existentes en el mismo.

3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se ha ejercido cualquiera de los poderes previstos en el presente artículo, así como toda información al respecto.

4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Sección 3. Jurisdicción

Artículo 22. Jurisdicción.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito previsto con arreglo a los artículos 2 a 11 del presente Convenio, siempre que se haya cometido:

a) En su territorio; o

b) a bordo de un buque que enarbole pabellón de dicha Parte; o

c) a bordo de una aeronave matriculada según las leyes de dicha Parte; o

d) por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar en el que se cometió o si ningún Estado tiene competencia territorial respecto del mismo.

2. Cualquier Estado podrá reservarse el derecho a no aplicar o a aplicar únicamente en determinados casos o condiciones las normas sobre jurisdicción establecidas en los apartados 1.b) a 1.d) del presente artículo o en cualquier otra parte de los mismos.

3. Cada Parte adoptará las medidas que resulten necesarias para afirmar su jurisdicción respecto de los delitos mencionados en el apartado 1 del artículo 24 del presente Convenio, cuando el presunto autor del delito se encuentre en su territorio y no pueda ser extraditado a otra Parte por razón de su nacionalidad, previa solicitud de extradición.

4. El presente Convenio no excluye ninguna jurisdicción penal ejercida por una Parte de conformidad con su derecho interno.

5. Cuando varias Partes reivindiquen su jurisdicción respecto de un presunto delito contemplado en el presente Convenio, las Partes interesadas celebrarán consultas, siempre que sea oportuno, con miras a determinar cuál es la jurisdicción más adecuada para las actuaciones penales.

CAPÍTULO III
Cooperación internacional

Sección 1. Principios generales

Título 1. Principios generales relativos a la cooperación internacional

Artículo 23. Principios generales relativos a la cooperación internacional.

Las Partes cooperarán entre sí en la mayor medida posible, de conformidad con las disposiciones del presente capítulo, en aplicación de los instrumentos internacionales aplicables a la cooperación internacional en materia penal, de acuerdos basados en legislación uniforme o recíproca y de su derecho interno, para los fines de las investigaciones o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para la obtención de pruebas electrónicas de los delitos.

Título 2. Principios relativos a la extradición

Artículo 24. Extradición.

1. a) El presente artículo se aplicará a la extradición entre las Partes por los delitos establecidos en los artículos 2 a 11 del presente Convenio, siempre que estén castigados en la legislación de las dos Partes implicadas con una pena privativa de libertad de una duración máxima de como mínimo un año, o con una pena más grave.

b) Cuando deba aplicarse una pena mínima diferente en virtud de un acuerdo basado en legislación uniforme o recíproca o de un tratado de extradición aplicable entre dos o más Partes, incluido el Convenio Europeo de Extradición (STE n.º 24), se aplicará la pena mínima establecida en virtud de dicho acuerdo o tratado.

2. Se considerará que los delitos mencionados en el apartado 1 del presente artículo están incluidos entre los delitos que dan lugar a extradición en cualquier tratado de extradición vigente entre las Partes. Las Partes se comprometen a incluir dichos delitos entre los que pueden dar lugar a extradición en cualquier tratado de extradición que puedan celebrar entre sí.

3. Cuando una Parte que condicione la extradición a la existencia de un tratado reciba una solicitud de extradición de otra Parte con la que no haya celebrado ningún tratado de extradición, podrá aplicar el presente Convenio como fundamento jurídico de la extradición respecto de cualquier delito mencionado en el apartado 1 del presente artículo.

4. Las Partes que no condicionen la extradición a la existencia de un tratado reconocerán los delitos mencionados en el apartado 1 del presente artículo como delitos que pueden dar lugar a extradición entre ellas.

5. La extradición estará sujeta a las condiciones establecidas en el derecho interno de la Parte requerida o en los tratados de extradición aplicables, incluidos los motivos por los que la Parte requerida puede denegar la extradición.

6. Cuando se deniegue la extradición por un delito mencionado en el apartado 1 del presente artículo únicamente por razón de la nacionalidad de la persona buscada o porque la Parte requerida se considera competente respecto de dicho delito, la Parte requerida deberá someter el asunto, a petición de la Parte requirente, a sus autoridades competentes para los fines de las actuaciones penales pertinentes, e informará a su debido tiempo del resultado final a la Parte requirente. Dichas autoridades tomarán su decisión y efectuarán sus investigaciones y procedimientos de la misma manera que para cualquier otro delito de naturaleza comparable, de conformidad con la legislación de dicha Parte.

7. a) Cada Parte comunicará al Secretario General del Consejo de Europa, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, el nombre y la dirección de cada autoridad responsable del envío o de la recepción de solicitudes de extradición o de detención provisional en ausencia de un tratado.

b) El Secretario General del Consejo de Europa creará y mantendrá actualizado un registro de las autoridades designadas por las Partes. Cada Parte garantizará en todo momento la exactitud de los datos que figuren en el registro.

Título 3. Principios generales relativos a la asistencia mutua

Artículo 25. Principios generales relativos a la asistencia mutua.

1. Las Partes se concederán asistencia mutua en la mayor medida posible para los fines de las investigaciones o procedimientos relativos a delitos relacionados con sistemas y datos informáticos o para la obtención de pruebas en formato electrónico de un delito.

2. Cada Parte adoptará también las medidas legislativas y de otro tipo que resulten necesarias para cumplir las obligaciones establecidas en los artículos 27 a 35.

3. En casos de urgencia, cada Parte podrá transmitir solicitudes de asistencia o comunicaciones relacionadas con las mismas por medios rápidos de comunicación, incluidos el fax y el correo electrónico, en la medida en que dichos medios ofrezcan niveles adecuados de seguridad y autenticación (incluido el cifrado, en caso necesario), con confirmación oficial posterior si la Parte requerida lo exige. La Parte requerida aceptará la solicitud y dará respuesta a la misma por cualquiera de estos medios rápidos de comunicación.

4. Salvo que se establezca específicamente otra cosa en los artículos del presente capítulo, la asistencia mutua estará sujeta a las condiciones previstas en el derecho

interno de la Parte requerida o en los tratados de asistencia mutua aplicables, incluidos los motivos por los que la Parte requerida puede denegar la cooperación. La Parte requerida no ejercerá el derecho a denegar la asistencia mutua en relación con los delitos mencionados en los artículos 2 a 11 únicamente porque la solicitud se refiere a un delito que considera de naturaleza fiscal.

5. Cuando, de conformidad con las disposiciones del presente capítulo, se permita a la Parte requerida condicionar la asistencia mutua a la existencia de una doble tipificación penal, dicha condición se considerará cumplida cuando la conducta constitutiva del delito respecto del cual se solicita la asistencia constituya un delito en virtud de su derecho interno, con independencia de que dicho derecho incluya o no el delito dentro de la misma categoría de delitos o lo denomine o no con la misma terminología que la Parte requirente,.

Artículo 26. Información espontánea.

1. Dentro de los límites de su derecho interno, y sin petición previa, una Parte podrá comunicar a otra Parte información obtenida en el marco de sus propias investigaciones cuando considere que la revelación de dicha información podría ayudar a la Parte receptora a iniciar o llevar a cabo investigaciones o procedimientos en relación con delitos previstos en el presente Convenio o podría dar lugar a una petición de cooperación de dicha Parte en virtud del presente capítulo.

2. Antes de comunicar dicha información, la Parte que la comunique podrá solicitar que se preserve su confidencialidad o que se utilice con sujeción a determinadas condiciones. Si la Parte receptora no puede atender esa solicitud, informará de ello a la otra Parte, que deberá entonces determinar si a pesar de ello debe facilitarse la información o no. Si la Parte destinataria acepta la información en las condiciones establecidas, quedará vinculada por las mismas.

Titulo 4. Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables

Artículo 27. Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables.

1. Cuando entre las Partes requirente y requerida no se encuentre vigente un tratado de asistencia mutua o un acuerdo basado en legislación uniforme o recíproca, serán de aplicación las disposiciones de los apartados 2 a 10 del presente artículo. Las disposiciones del presente artículo no serán de aplicación cuando exista un tratado, acuerdo o legislación de este tipo, salvo que las Partes interesadas convengan en aplicar en su lugar la totalidad o una parte del resto del presente artículo.

2. a) Cada Parte designará una o varias autoridades centrales encargadas de enviar solicitudes de asistencia mutua y de dar respuesta a las mismas, de su ejecución y de su remisión a las autoridades competentes para su ejecución.

b) Las autoridades centrales se comunicarán directamente entre sí.

c) En el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, cada Parte comunicará al Secretario General del Consejo de Europa los nombres y direcciones de las autoridades designadas en cumplimiento del presente apartado.

d) El Secretario General del Consejo de Europa creará y mantendrá actualizado un registro de las autoridades centrales designadas por las Partes. Cada Parte garantizará en todo momento la exactitud de los datos que figuren en el registro.

3. Las solicitudes de asistencia mutua en virtud del presente artículo se ejecutarán de conformidad con los procedimientos especificados por la Parte requirente, salvo que sean incompatibles con la legislación de la Parte requerida.

4. Además de las condiciones o de los motivos de denegación contemplados en el apartado 4 del artículo 25, la Parte requerida podrá denegar la asistencia si:

a) La solicitud se refiere a un delito que la Parte requerida considera delito político o delito vinculado a un delito político;

b) la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.

5. La Parte requerida podrá posponer su actuación en respuesta a una solicitud cuando dicha actuación pudiera causar perjuicios a investigaciones o procedimientos llevados a cabo por sus autoridades.

6. Antes de denegar o posponer la asistencia, la Parte requerida estudiará, previa consulta cuando proceda con la Parte requirente, si puede atenderse la solicitud parcialmente o con sujeción a las condiciones que considere necesarias.

7. La Parte requerida informará sin demora a la Parte requirente del resultado de la ejecución de una solicitud de asistencia. Deberá motivarse cualquier denegación o aplazamiento de la asistencia solicitada. La Parte requerida informará también a la Parte requirente de cualquier motivo que haga imposible la ejecución de la solicitud o que pueda retrasarla de forma significativa.

8. La Parte requirente podrá solicitar a la Parte requerida que preserve la confidencialidad de la presentación de una solicitud en virtud del presente capítulo y del objeto de la misma, salvo en la medida necesaria para su ejecución. Si la Parte requerida no puede cumplir esta petición de confidencialidad, lo comunicará inmediatamente a la Parte requirente, que determinará entonces si pese a ello debe procederse a la ejecución de la solicitud.

9. a) En casos de urgencia, las solicitudes de asistencia mutua o las comunicaciones al respecto podrán ser enviadas directamente por las autoridades judiciales de la Parte requirente a las autoridades correspondientes de la Parte requerida. En tal caso, se enviará al mismo tiempo copia a la autoridad central de la Parte requerida a través de la autoridad central de la Parte requirente.

b) Cualquier solicitud o comunicación en virtud de este apartado podrá efectuarse a través de la Organización Internacional de Policía Criminal (INTERPOL).

c) Cuando se presente una solicitud en aplicación de la letra a) del presente artículo y la autoridad no sea competente para tramitarla, remitirá la solicitud a la autoridad nacional competente e informará directamente a la Parte requirente de dicha remisión.

d) Las solicitudes y comunicaciones efectuadas en virtud del presente apartado que no impliquen medidas coercitivas podrán ser remitidas directamente por las autoridades competentes de la Parte requirente a las autoridades competentes de la Parte requerida.

e) En el momento de la firma o el depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, cada Parte podrá informar al Secretario General del

Consejo de Europa de que, por razones de eficacia, las solicitudes formuladas en virtud del presente apartado deberán dirigirse a su autoridad central.

Artículo 28. Confidencialidad y restricción de la utilización.

1. En ausencia de un tratado de asistencia mutua o de un acuerdo basado en legislación uniforme o recíproca que esté vigente entre las Partes requirente y requerida, serán de aplicación las disposiciones del presente artículo. Las disposiciones del presente artículo no serán de aplicación cuando exista un tratado, acuerdo o legislación de este tipo, salvo que las Partes interesadas convengan en aplicar en su lugar la totalidad o una parte del resto del presente artículo.

2. La Parte requerida podrá supeditar la entrega de información o material en respuesta a una solicitud a la condición de que:

a) Se preserve su confidencialidad cuando la solicitud de asistencia judicial mutua no pueda ser atendida en ausencia de esta condición, o

b) no se utilicen para investigaciones o procedimientos distintos de los indicados en la solicitud.

3. Si la Parte requirente no puede cumplir alguna condición de las mencionadas en el apartado 2, informará de ello sin demora a la otra Parte, que determinará en tal caso si pese a ello debe facilitarse la información. Cuando la Parte requirente acepte la condición, quedará vinculada por ella.

4. Cualquier Parte que facilite información o material con sujeción a una condición con arreglo a lo dispuesto en el apartado 2 podrá requerir a la otra Parte que explique, en relación con dicha condición, el uso dado a dicha información o material.

Sección 2. Disposiciones especiales

Título 1. Asistencia mutua en materia de medidas provisionales

Artículo 29. Conservación rápida de datos informáticos almacenados.

1. Una Parte podrá solicitar a otra Parte que ordene o asegure de otra forma la conservación rápida de datos almacenados por medio de un sistema informático que se encuentre en el territorio de esa otra Parte, respecto de los cuales la Parte requirente tenga la intención de presentar una solicitud de asistencia mutua con vistas al registro o al acceso de forma similar, la confiscación o la obtención de forma similar, o la revelación de los datos.

2. En las solicitudes de conservación que se formulen en virtud del apartado 1 se indicará:

a) La autoridad que solicita dicha conservación;

b) el delito objeto de investigación o de procedimiento penal y un breve resumen de los hechos relacionados con el mismo;

c) los datos informáticos almacenados que deben conservarse y su relación con el delito;

d) cualquier información disponible que permita identificar a la persona encargada de la custodia de los datos informáticos almacenados o la ubicación del sistema informático;

e) la necesidad de la conservación; y

f) que la Parte tiene la intención de presentar una solicitud de asistencia mutua para el registro o el acceso de forma similar, la confiscación o la obtención de forma similar o la revelación de los datos informáticos almacenados.

3. Tras recibir la solicitud de otra Parte, la Parte requerida tomará las medidas adecuadas para conservar rápidamente los datos especificados de conformidad con su derecho interno. A los efectos de responder a una solicitud, no se requerirá la doble tipificación penal como condición para proceder a la conservación.

4. Cuando una Parte exija la doble tipificación penal como condición para atender una solicitud de asistencia mutua para el registro o el acceso de forma similar, la confiscación o la obtención de forma similar o la revelación de datos almacenados, dicha Parte podrá reservarse, en relación con delitos distintos de los previstos con arreglo a los artículos 2 a 11 del presente Convenio, el derecho a denegar la solicitud de conservación en virtud del presente artículo en los casos en que tenga motivos para creer que la condición de la doble tipificación penal no podrá cumplirse en el momento de la revelación.

5. Asimismo, las solicitudes de conservación únicamente podrán denegarse si:

a) La solicitud hace referencia a un delito que la Parte requerida considera delito político o delito relacionado con un delito político;

b) la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.

6. Cuando la Parte requerida considere que la conservación por sí sola no bastará para garantizar la futura disponibilidad de los datos o pondrá en peligro la confidencialidad de la investigación de la Parte requirente o causará cualquier otro perjuicio a la misma, informará de ello sin demora a la Parte requirente, la cual decidirá entonces si debe pese a ello procederse a la ejecución de la solicitud.

7. Las medidas de conservación adoptadas en respuesta a la solicitud mencionada en el apartado 1 tendrán una duración mínima de sesenta días, con objeto de permitir a la Parte requirente presentar una solicitud de registro o de acceso de forma similar, confiscación u obtención de forma similar, o de revelación de los datos. Cuando se reciba dicha solicitud, seguirán conservándose los datos hasta que se adopte una decisión sobre la misma.

Artículo 30. Revelación rápida de datos conservados sobre el tráfico.

1. Cuando, con motivo de la ejecución de una solicitud presentada de conformidad con el artículo 29 para la conservación de datos sobre el tráfico en relación con una comunicación específica, la Parte requerida descubra que un proveedor de servicios de otro Estado participó en la transmisión de la comunicación, la Parte requerida revelará rápidamente a la Parte requirente un volumen suficiente de datos sobre el tráfico para identificar al proveedor de servicios y la vía por la que se transmitió la comunicación.

2. La revelación de datos sobre el tráfico en virtud del apartado 1 únicamente podrá denegarse si:

a) La solicitud hace referencia a un delito que la Parte requerida considera delito político o delito relacionado con un delito político;

b) la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.

Título 2. Asistencia mutua en relación con los poderes de investigación

Artículo 31. Asistencia mutua en relación con el acceso a datos informáticos almacenados.

1. Una Parte podrá solicitar a otra Parte que registre o acceda de forma similar, confisque u obtenga de forma similar y revele datos almacenados por medio de un sistema informático situado en el territorio de la Parte requerida, incluidos los datos conservados en aplicación del artículo 29.

2. La Parte requerida dará respuesta a la solicitud aplicando los instrumentos internacionales, acuerdos y legislación mencionados en el artículo 23, así como de conformidad con otras disposiciones aplicables en el presente capítulo.

3. Se dará respuesta lo antes posible a la solicitud cuando:

a) Existan motivos para creer que los datos pertinentes están especialmente expuestos al riesgo de pérdida o modificación; o

b. los instrumentos, acuerdos o legislación mencionados en el apartado 2 prevean la cooperación rápida.

Artículo 32. Acceso transfronterizo a datos almacenados, con consentimiento o cuando estén a disposición del público.

Una Parte podrá, sin la autorización de otra Parte:

a) Tener acceso a datos informáticos almacenados que se encuentren a disposición del público (fuente abierta), con independencia de la ubicación geográfica de dichos datos; o

b) tener acceso o recibir, a través de un sistema informático situado en su territorio, datos informáticos almacenados situados en otra Parte, si la Parte obtiene el consentimiento lícito y voluntario de la persona legalmente autorizada para revelar los datos a la Parte por medio de ese sistema informático.

Artículo 33. Asistencia mutua para la obtención en tiempo real de datos sobre el tráfico.

1. Las Partes se prestarán asistencia mutua para la obtención en tiempo real de datos sobre el tráfico asociados a comunicaciones específicas en su territorio transmitidas por medio de un sistema informático. Con sujeción a lo dispuesto en el apartado 2, dicha asistencia se regirá por las condiciones y procedimientos establecidos en el derecho interno.

2. Cada Parte prestará dicha asistencia como mínimo respecto de los delitos por los que se podría conseguir la obtención en tiempo real de datos sobre el tráfico en un caso similar en su país.

Artículo 34. Asistencia mutua relativa a la interceptación de datos sobre el contenido.

Las Partes se prestarán asistencia mutua para la obtención o grabación en tiempo real de datos sobre el contenido de comunicaciones específicas transmitidas por medio de un sistema informático en la medida en que lo permitan sus tratados y el derecho interno aplicables.

Título 3. Red 24/7

Artículo 35. Red 24/7.

1. Cada Parte designará un punto de contacto disponible las veinticuatro horas del día, siete días a la semana, con objeto de garantizar la prestación de ayuda inmediata para los fines de las investigaciones o procedimientos relacionados con delitos vinculados a sistemas y datos informáticos, o para la obtención de pruebas electrónicas de un delito. Dicha asistencia incluirá los actos tendentes a facilitar las siguientes medidas o su adopción directa, cuando lo permitan la legislación y la práctica internas:

a) El asesoramiento técnico;

b) la conservación de datos en aplicación de los artículos 29 y 30;

c) la obtención de pruebas, el suministro de información jurídica y la localización de sospechosos.

2. a) El punto de contacto de una Parte estará capacitado para mantener comunicaciones con el punto de contacto de otra Parte con carácter urgente.

b) Si el punto de contacto designado por una Parte no depende de la autoridad o de las autoridades de dicha Parte responsables de la asistencia mutua internacional o de la extradición, el punto de contacto velará por garantizar la coordinación con dicha autoridad o autoridades con carácter urgente.

3. Cada Parte garantizará la disponibilidad de personal debidamente formado y equipado con objeto de facilitar el funcionamiento de la red.

CAPÍTULO IV
Disposiciones finales

Artículo 36. Firma y entrada en vigor.

1. El presente Convenio estará abierto a la firma de los Estados miembros del Consejo de Europa y de los Estados no miembros que hayan participado en su elaboración.

2. El presente Convenio estará sujeto a ratificación, aceptación o aprobación. Los instrumentos de ratificación, aceptación o aprobación se depositarán en poder del Secretario General del Consejo de Europa.

3. El presente Convenio entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que cinco Estados, de los cuales tres como mínimo sean Estados miembros del Consejo de Europa, hayan expresado su consentimiento para quedar vinculados por el Convenio de conformidad con lo dispuesto en los apartados 1 y 2.

4. Respecto de cualquier Estado signatario que exprese más adelante su consentimiento para quedar vinculado por el Convenio, éste entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que haya expresado su consentimiento para quedar vinculado por el Convenio de conformidad con lo dispuesto en los apartados 1 y 2.

Artículo 37. Adhesión al Convenio.

1. Tras la entrada en vigor del presente Convenio, el Comité de Ministros del Consejo de Europa, previa consulta con los Estados Contratantes del Convenio y una vez obtenido su consentimiento unánime, podrá invitar a adherirse al presente Convenio a cualquier Estado que no sea miembro del Consejo y que no haya participado en su elaboración. La decisión se adoptará por la mayoría establecida en el artículo 20.d) del Estatuto del Consejo de Europa y con el voto unánime de los representantes con derecho a formar parte del Comité de Ministros.

2. Para todo Estado que se adhiera al Convenio de conformidad con lo dispuesto en el anterior apartado 1, el Convenio entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha del depósito del instrumento de adhesión en poder del Secretario General del Consejo de Europa.

Artículo 38. Aplicación territorial.

1. En el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, cada Estado podrá especificar el territorio o territorios a los que se aplicará el presente Convenio.

2. En cualquier momento posterior, mediante declaración dirigida al Secretario General del Consejo de Europa, cualquier Parte podrá hacer extensiva la aplicación del presente Convenio a cualquier otro territorio especificado en la declaración. Respecto de dicho territorio, el Convenio entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido la declaración.

3. Toda declaración formulada en virtud de los dos apartados anteriores podrá retirarse, respecto de cualquier territorio especificado en la misma, mediante notificación dirigida al Secretario General del Consejo de Europa. La retirada surtirá efecto el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido dicha notificación.

Artículo 39. Efectos del Convenio.

1. La finalidad del presente Convenio es completar los tratados o acuerdos multilaterales o bilaterales aplicables entre las Partes, incluidas las disposiciones de:

– El Convenio europeo de extradición, abierto a la firma en París el 13 de diciembre de 1957 (STE n.º 24);

– el Convenio europeo de asistencia judicial en materia penal, abierto a la firma en Estrasburgo el 20 de abril de 1959 (STE n.º 30);

– el Protocolo adicional al Convenio europeo de asistencia judicial en materia penal, abierto a la firma en Estrasburgo el 17 de marzo de 1978 (STE n.º 99).

2. Si dos o más Partes han celebrado ya un acuerdo o tratado sobre las materias reguladas en el presente Convenio o han regulado de otra forma sus relaciones al respecto, o si lo hacen en el futuro, tendrán derecho a aplicar, en lugar del presente Convenio, dicho acuerdo o tratado o a regular dichas relaciones en consonancia. No obstante, cuando las Partes regulen sus relaciones respecto de las materias contempladas en el presente Convenio de forma distinta a la establecida en el mismo, deberán hacerlo de una forma que no sea incompatible con los objetivos y principios del Convenio.

3. Nada de lo dispuesto en el presente Convenio afectará a otros derechos, restricciones, obligaciones y responsabilidades de las Partes.

Artículo 40. Declaraciones.

Mediante notificación por escrito dirigida al Secretario General del Consejo de Europa, cualquier Estado podrá declarar, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, que se acoge a la facultad de exigir elementos complementarios según lo dispuesto en los artículos 2, 3, 6.1.b), 7, 9.3 y 27.9.e).

Artículo 41. Cláusula federal.

1. Los Estados federales podrán reservarse el derecho a asumir las obligaciones derivadas del capítulo II del presente Convenio de forma compatible con los principios fundamentales por los que se rija la relación entre su gobierno central y los estados que lo formen u otras entidades territoriales análogas, siempre que siga estando en condiciones de cooperar de conformidad con el capítulo III.

2. Cuando formule una reserva en aplicación del apartado 1, un Estado federal no podrá aplicar los términos de dicha reserva para excluir o reducir sustancialmente sus obligaciones en relación con las medidas contempladas en el capítulo II. En todo caso, deberá dotarse de una capacidad amplia y efectiva que permita la aplicación de las medidas previstas en dicho capítulo.

3. Por lo que respecta a las disposiciones del presente Convenio cuya aplicación sea competencia de los estados federados o de otras entidades territoriales análogas que no estén obligados por el sistema constitucional de la federación a la adopción de medidas legislativas, el gobierno federal informará de esas disposiciones a las autoridades competentes de dichos estados, junto con su opinión favorable, alentándoles a adoptar las medidas adecuadas para su aplicación.

Artículo 42. Reservas.

Mediante notificación por escrito dirigida al Secretario General del Consejo de Europa, cualquier Estado podrá declarar, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, que se acoge a una o varias de las reservas previstas en el apartado 2 del artículo 4, apartado 3 del artículo 6, apartado 4 del artículo 9, apartado 3 del artículo 10, apartado 3 del artículo 11, apartado 3 del artículo 14, apartado 2 del artículo 22, apartado 4 del artículo 29 y apartado 1 del artículo 41. No podrán formularse otras reservas.

Artículo 43. Situación de las reservas y retirada de las mismas.

1. La Parte que haya formulado una reserva de conformidad con el artículo 42 podrá retirarla en todo o en parte mediante notificación dirigida al Secretario General del Consejo de Europa. Dicha retirada surtirá efecto en la fecha en que el Secretario General reciba la notificación. Si en la notificación se indica que la retirada de una reserva surtirá efecto en una fecha especificada en la misma y ésta es posterior a la fecha en que el Secretario General reciba la notificación, la retirada surtirá efecto en dicha fecha posterior.

2. La Parte que haya formulado una reserva según lo dispuesto en el artículo 42 retirará dicha reserva, en todo o en parte, tan pronto como lo permitan las circunstancias.

3. El Secretario General del Consejo de Europa podrá preguntar periódicamente a las Partes que hayan formulado una o varias reservas según lo dispuesto en el artículo 42 acerca de las perspectivas de que se retire dicha reserva.

Artículo 44. Enmiendas.

1. Cualquier Estado Parte podrá proponer enmiendas al presente Convenio, que serán comunicadas por el Secretario General del Consejo de Europa a los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del presente Convenio así como a cualquier Estado que se haya adherido al presente Convenio o que haya sido invitado a adherirse al mismo de conformidad con lo dispuesto en el artículo 37.

2. Las enmiendas propuestas por una Parte serán comunicadas al Comité Europeo de Problemas Penales (CDPC), que presentará al Comité de Ministros su opinión sobre la enmienda propuesta.

3. El Comité de Ministros examinará la enmienda propuesta y la opinión presentada por el CDPC y, previa consulta con los Estados Partes no miembros en el presente Convenio, podrá adoptar la enmienda.

4. El texto de cualquier enmienda adoptada por el Comité de Ministros de conformidad con el apartado 3 del presente artículo será remitido a las Partes para su aceptación.

5. Cualquier enmienda adoptada de conformidad con el apartado 3 del presente artículo entrará en vigor treinta días después de que las Partes hayan comunicado su aceptación de la misma al Secretario General.

Artículo 45. Solución de controversias.

1. Se mantendrá informado al Comité Europeo de Problemas Penales del Consejo de Europa (CDPC) acerca de la interpretación y aplicación del presente Convenio.

2. En caso de controversia entre las Partes sobre la interpretación o aplicación del presente Convenio, éstas intentarán resolver la controversia mediante negociaciones o por cualquier otro medio pacífico de su elección, incluida la sumisión de la controversia al CDPC, a un tribunal arbitral cuyas decisiones serán vinculantes para las Partes o a la Corte Internacional de Justicia, según acuerden las Partes interesadas.

Artículo 46. Consultas entre las Partes.

1. Las Partes se consultarán periódicamente, según sea necesario, con objeto de facilitar:

a) La utilización y la aplicación efectivas del presente Convenio, incluida la detección de cualquier problema derivado del mismo, así como los efectos de cualquier declaración o reserva formulada de conformidad con el presente Convenio;

b) el intercambio de información sobre novedades significativas de carácter jurídico, político o tecnológico relacionadas con la ciberdelincuencia y con la obtención de pruebas en formato electrónico;

c) el estudio de la conveniencia de ampliar o enmendar el presente Convenio.

2. Se mantendrá periódicamente informado al Comité Europeo de Problemas Penales (CDPC) acerca del resultado de las consultas mencionadas en el apartado 1.

3. Cuando proceda, el CDPC facilitará las consultas mencionadas en el apartado 1 y tomará las medidas necesarias para ayudar a las Partes en sus esfuerzos por ampliar o enmendar el Convenio. Como máximo tres años después de la entrada en vigor del presente Convenio, el Comité Europeo de Problemas Penales (CDPC) llevará a cabo, en cooperación con las Partes, una revisión de todas las disposiciones del Convenio y, en caso necesario, recomendará las enmiendas procedentes.

4. Salvo en los casos en que sean asumidos por el Consejo de Europa, los gastos realizados para aplicar lo dispuesto en el apartado 1 serán sufragados por las Partes en la forma que éstas determinen.

5. Las Partes contarán con la asistencia de la Secretaría del Consejo de Europa para desempeñar sus funciones en aplicación del presente artículo.

Artículo 47. Denuncia.

1. Cualquier Parte podrá denunciar en cualquier momento el presente Convenio mediante notificación dirigida al Secretario General del Consejo de Europa.

2. Dicha denuncia surtirá efecto el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido la notificación.

Artículo 48. Notificación.

El Secretario General del Consejo de Europa notificará a los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del presente Convenio y a cualquier Estado que se haya adherido al mismo o que haya sido invitado a hacerlo:

a) Cualquier firma;

b) el depósito de cualquier instrumento de ratificación, aceptación, aprobación o adhesión;

c) cualquier fecha de entrada en vigor del presente Convenio de conformidad con los artículos 36 y 37;

d) cualquier declaración formulada en virtud del artículo 40 o reserva formulada de conformidad con el artículo 42;

e) cualquier otro acto, notificación o comunicación relativo al presente Convenio.

En fe de lo cual, los infrascritos, debidamente autorizados a tal fin, firman el presente Convenio.

Hecho en Budapest, el 23 de noviembre de 2001, en francés e inglés, siendo ambos textos igualmente auténticos, en un ejemplar único que se depositará en los archivos del Consejo de Europa. El Secretario General del Consejo de Europa remitirá copias certificadas a cada uno de los Estados Miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del presente Convenio y a cualquier Estado invitado a adherirse al mismo.


ITU