ESTUDIO DE UNA ADHESIÓN DE COLOMBIA AL CONVENIO DE BUDAPEST, VISTO DESDE LA LEGISLACIÓN Y SEGURIDAD INFORMÁTICA

WILLIAM MARTINEZ CAMARGO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS Y TECNOLOGIA E INGENIERIA
ESPECILIZACION EN SEGURIDAD INFORMATICA
BOGOTA
2017

ESTUDIO DE UNA ADHESIÓN DE COLOMBIA AL CONVENIO DE BUDAPEST, VISTO DESDE LA LEGISLACIÓN Y SEGURIDAD INFORMÁTICA

WILLIAM MARTINEZ CAMARGO

Monografía para optar al título de
Especialista en Seguridad Informática

Asesor
Mag. Esp. Ing. Francisco Solarte

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
BOGOTA
2017

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá, 28 noviembre 2017

DEDICATORIA

A Dios que me permitió lograr llegar a este punto de mi vida con esfuerzo, mucha compañía y amor.

A mi familia y amigos que, aunque son pocos siempre me han enseñado el valor de nunca rendirme y siempre escalar un peldaño más.

A mis hijos que siempre son la fuente de inspiración inagotable en el hermoso camino de nunca dejar de aprender.

William Martínez

AGRADECIMIENTOS

A Dios por haberme permitido llegar a estas instancias y entregarme la sabiduría suficiente para no desfallecer.

A mis hijos que cada día me enseñan algo nuevo, a mis amadas madres que todo el tiempo me han apoyado, a mi esposa por ser un soporte todo el tiempo, a mi hermano por sus valiosos comentarios y consejos.

A mi director de grado por sus aportes, esmero en la formación y acompañamiento en el desarrollo de este trabajo.

A los ingenieros Manuel Antonio Sierra Rodríguez, Salomón Rodríguez y Francisco Antonio Solarte quienes en todo momento me brindaron sus conocimientos y valiosas contribuciones en la comprensión y buen desarrollo de mi proyecto.

CONTENIDO

LISTA DE TABLAS

Pág.

LISTA DE GRÁFICAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

GLOSARIO

ADHESION A UN CONVENIO: proceso mediante el cual un país debe cumplir unos parámetros y requerimientos para pertenecer a un convenio.

CONVENIO CIBERDELINCUENCIA BUDAPEST: Conocido también como “convenio de ciberdelincuencia” es un acuerdo de carácter internacional, único en su género en el mundo entero, el cual se basa en la cooperación internacional, el derecho procesal y penal para luchar contra los delitos de carácter informático tipificados en sus artículos. Se firmó el 23 de noviembre de 2001 y comenzó a operar en el año 2004.

DELITO INFORMATICO: es la conducta de carácter ilícito (acción u omisión) de cualquier ciudadano, que mediante el uso de sistemas informáticos comete un delito con el cual afecta a otra(s) persona(s), a sus bienes, a un estado o a una entidad jurídica.

LEGISLACION INFORMATICA: conjunto de leyes, procesos y procedimientos creados para reglamentar todo en materia informática.

COMPES: documento que se expide por el Consejo Nacional de Política Económica y Social el cual se encarga de estudiar todo tipo de política relacionada a estos temas.

RESUMEN

El mundo nunca antes había sido tan tecnológico, y es mucho lo que espera a las nuevas generaciones en esta materia. Los países crecen en forma desigual y los avances tecnológicos no tiene presente esto; el afán por vender y consumir todo tipo de aparatos tecnológicos, está dejando al descubierto la gran necesidad de capacitación sobre seguridad informática, a todo nivel.

Con el desmesurado avance en la creación de nueva tecnología, aparecieron palabras como ciberdelito, ciberdelincuencia, ciberdefensa y tantas otras, que permite evidenciar, que el mundo evoluciona de forma más dinámica y que cada segundo que pasa, el planeta entero se expone a un mayor riesgo; es entonces, cuando surgen preguntas como: ¿es tal vez el momento oportuno para que el mundo entero se una, con el fin de hacer frente a la gran amenaza del ciberdelito?, ¿realmente necesita Colombia pertenecer al convenio de ciberdelincuencia de Budapest?, ¿necesita el país realizar grandes cambios para lograr una verdadera adhesión al convenio de ciberseguridad de Budapest?

El presente documento, muestra información de la investigación realizada sobre el convenio de Ciberdelincuencia de Budapest, en el que se podrán apreciar, los antecedentes, el marco jurídico existente, los actores del convenio, su normatividad y tendencias; en lo concerniente a Colombia, se efectuó una revisión de la legislación en materia de seguridad informática, el estado actual, sus falencias y necesidades a futuro.

El alcance del documento, es el de generar una propuesta para la adhesión de Colombia al convenio en ciberdelincuencia de Budapest, por esta razón el estudio parte de una contextualización y estudio de las diferentes variables, escenarios que se ven y verán comprometidos en el marco de una eventual adhesión al convenio.

PALABRAS CLAVE: Convenio de ciberdelincuencia de Budapest, legislación informática, Ley 1273 de 2009, Ciberdelincuencia, Ciberdelito, Ciberdefensa, Ciberespacio, Ciberterrorismo.

INTRODUCCIÓN

El propósito del documento final, es generar conocimiento a través de una propuesta que sirva de base a futuros estudios, los cuales establezcan un punto de referencia sobre la importancia, ventajas y desventajas de la adhesión de un país como Colombia al convenio de Budapest.

Partiendo de una conceptualización y unos antecedentes, donde el lector podrá identificar el camino que llevó a los países del continente europeo a la creación del convenio de ciberseguridad, al igual, que los países que al momento se encuentran adheridos, se realizara una tipificación de cada uno de estos países.

En el apartado siguiente, se presenta el estado actual de los países adheridos y los requerimientos que han debido cumplir para lograr un buen proceso de adhesión. Posteriormente, se verá la proyección a futuro de cada uno de los países ya incluidos.

Para el final, se encontrará las tendencias que podría presentar Colombia en el marco de una posible adhesión, teniendo en cuenta lo sucedido en otros países.

1. PLANTEAMIENTO DEL PROBLEMA

La seguridad informática se convierte cada día en un área de estudio muy poderosa y de gran necesidad, debido a que personas inescrupulosas hacen uso incorrecto tanto de la tecnología, como de la información, generando un sin número de problemas para los Estados y sus habitantes, razones suficientes que han motivado y consolidado en varios países, el desarrollo legal en esta materia para frenar toda clase de acciones que atenta indiscriminadamente, a los derechos de personas naturales y jurídicas.

1.1 DEFINICIÓN DEL PROBLEMA

Cuando se habla del convenio de Budapest, muchas personas involucradas en el estudio de la seguridad informática, entienden que se refieren a un documento que versa sobre la ciberdelincuencia; sin embargo, al preguntarles, si es beneficioso o no para un país como Colombia adherirse a este convenio, la mayoría de ellos no tienen claro si es favorable o no.

Actualmente no existe documentación que exponga las ventajas o desventajas que represente vincularse al citado Convenio, o que simplemente de una señal de partida sobre lo que pueda llegar a ser. Desde este punto de vista, se hace necesario la realización de un documento que ilustre sobre, este acuerdo internacional, la regulación colombiana en el ámbito de seguridad informática y de luces sobre lo que podría ocurrir en el evento de aceptar la aplicación en Colombia de este convenio, reflejando diversos escenarios que se pueden presentar, no propiamente jurídicos, y que son de particular importancia.

Colombia viene trabajando desde hace ya varios años en materia de seguridad informática, ciberdelincuencia y ciberdefensa; muestra de ello es la expedición de normas sobre el tema en cuestión, entre las que figura la Ley 527 de 1999, Ley 299 de 2000, Ley 962 de 2005, Ley 1341 de 2009 y muchas otras, que serán vistas en el texto, al igual que el documento CONPES 3701 del año 2011.

Sin embargo, para avanzar en la regulación de la seguridad informática, es imperativo comprender que al adherirse a un tratado de carácter internacional, Colombia tendrá que cumplir con una cantidad de requisitos en materia legislativa, así como disponer de recursos económicos, educativos y de capacitación e infraestructura, entre otros.

Es necesario que el Gobierno colombiano y sus habitantes, comprenda la importancia, derechos, deberes y obligaciones, que implica la aceptación de un convenio internacional de tal magnitud, y en esta medida será útil un documento que se dedique a ilustrarlo.

1.2 FORMULACION DEL PROBLEMA

¿Cómo puede contribuir el estudio documental sobre el convenio de Ciberdelincuencia de Budapest, en el planteamiento de una propuesta para determinar las ventajas y desventajas de la adhesión de Colombia, a dicho acuerdo internacional?

1.3 OBJETIVOS

1.3.1 Objetivo general

Presentar una propuesta integral para determinar las condiciones que debe cumplir un país como Colombia, en la adhesión al convenio de Ciberdelincuencia de Budapest, a través de un estudio documental comparativo que muestre las ventajas y desventajas de dicha adhesión.

1.3.2 Objetivos específicos

- Realizar el levantamiento de información conceptual referente al convenio de ciberdelincuencia de Budapest, marco jurídico existente y antecedentes.
- Determinar el alcance del convenio de ciberdelincuencia, los actores del convenio, legislación existente en materia de seguridad informática en Colombia, requerimientos para la adhesión al convenio, normatividad que rige y tendencias ante una posible adhesión.
- Plantear una propuesta para los cumplimientos de adhesión al tratado Budapest teniendo presente el estado actual por parte de Colombia.

1.4 JUSTIFICACIÓN

Si bien es cierto que Colombia ha realizado méritos para ser invitado a adherirse al Convenio de ciberdelincuencia (lo cual venía trabajando desde el año 2011 con la elaboración del CONPES 3701), también es claro, que no muchas personas comprenden la trascendencia o problemática que puede conllevar la realización de esta adhesión. De igual forma, al consultar información en línea y en bibliotecas, no hay evidencia de las ventajas o desventajas que esta puede generar, la información es mínima o inexistente y no hay un análisis desde el punto de vista de la seguridad informática.

El convenio de Budapest o de ciberdelincuencia, como es más conocido, fue establecido cuando ya existían otros convenios de cooperación en Europa, en materia penal, partiendo de la necesidad de unir esfuerzos para la lucha contra los delitos de carácter informático en el continente europeo, contando además, con la presencia de países observadores como Canadá, Japón y China, de los cuales posteriormente, se adhirieron los dos primeros Estados. En la actualidad, se espera que países como Costa Rica, Chile, Uruguay, Colombia y otros, tengan esa misma posibilidad.

Este Proyecto busca comprender que es el convenio de ciberdelincuencia, mostrar su importancia y dar a todos aquellos interesados en la seguridad informática, una idea de los beneficios o daños que puede llegar a causar para Colombia; al final, generara una propuesta para la adhesión de Colombia al convenio de Ciberdelincuencia de Budapest, el cual se espera sea también un documento base para posteriores estudios, análisis o consultas partiendo de información bibliográfica tan importante como el convenio de Budapest, la Constitución Política de Colombia leyes colombianas en materia de seguridad informática, y demás libros y artículos sobre el tema.

1.5 ALCANCE Y DELIMITACION DEL PROYECTO

1.5.1 Alcance. El documento pretende formular una propuesta para la adhesión de Colombia al convenio en ciberdelincuencia de Budapest, por esta razón, el estudio parte de una contextualización y revisión de las diferentes variables, escenarios que se ven y verán comprometidos, en el marco de una eventual adhesión al. acuerdo internacional.

A partir de esta contextualización, se genera una propuesta que permita servir de documento base para posteriores estudios que den luces sobre las ventajas y desventajas de la adhesión de Colombia o incluso otros países, a dicho convenio.

El proceso de investigación realizado busca abarcar de forma integral, diferentes planos y está dirigido a ser un documento de consulta para estudiosos del tema y personal vinculado a la seguridad informática en el mundo.

1.5.2 Delimitaciones. Esta monografía no busca modificar, ni cambiar ningún tipo de legislación, ni ser un documento norma, por el contrario, busca despertar el cuestionamiento y comprensión de las limitantes y fortalezas que puede tener un país en materia de seguridad informática, al momento de tomar la decisión de adherirse al convenio de ciberdelincuencia de Budapest.

1.6 DISEÑO METODOLOGICO

1.6.1 Tipo de investigación. Investigación de carácter Bibliográfico y documental, basada en la recolección, selección y análisis de documentos, con la utilización de procedimientos de carácter lógico y mental como el análisis, síntesis, deducción e inducción, que permiten la generación de una nueva propuesta a través de la presentación de resultados.

Se toma como fundamento, los conocimientos y criterios correspondientes al convenio de ciberdelincuencia, la seguridad informática y los parámetros legislativos en Colombia y la unión europea, al igual que de los países ya adheridos.

1.6.2 Diseño de la investigación. El desarrollo de toda investigación conlleva un plan detallado y pormenorizado, que en esta ocasión se adelantó así:

- ✓ Levantamiento de información y generación de conceptualización
- ✓ Generación de antecedentes que muestran al lector, el camino que condujo al convenio de Budapest, su creación, variables que le dieron adhesión a los países miembros, y países adheridos, brindando una tipificación de estos.
- ✓ Presentación del estado actual de los países adheridos y Colombia.
- ✓ Elaboración y determinación de la proyección a futuro.
- ✓ Tendencias del Estado Colombiano ante la posibilidad de aceptar la aplicación del acuerdo internacional, acorde con la experiencia de otros países.
- ✓ Análisis y elaboración de la propuesta.

1.6.3 Métodos y técnicas de recolección de información. Para cumplir con los objetivos y el plan diseñado se realizó consulta bibliográfica a través de documentos físicos y electrónicos como:

- ✓ Libros: Consultados directamente en bibliotecas como la Luis Ángel Arango, Julio Mario Santo Domingo, Virgilio Barco y en internet a través de la biblioteca virtual de la Universidad Nacional Abierta y a Distancia UNAD.
- ✓ Publicaciones Periódicas: Como jurisprudencia, leyes, normas.
- ✓ Documentos electrónicos: Consultas en internet alusivas a revistas, periódicos, artículos científicos de bases de datos, documentos oficiales y portales como el del Consejo de Europa.

1.6.4 Métodos y técnicas de análisis. Al finalizar la consulta y registro de información se efectuó el análisis documental de forma objetiva, extrayendo la información necesaria para poder realizar la comparación, análisis crítico, resúmenes y generación de una propuesta que permita brindar conocimiento y valor agregado a todo aquel que la consulte.

1.6.5 Materiales. Consulta bibliográfica, documentos online, material de biblioteca, artículos, revistas, documentos oficiales, normas legales, software office, equipo de cómputo, etc.

2. MARCO REFERENCIAL

La aparición de Internet, cambio la vida de todos los seres humanos en lo social, económico, cultural, educativo, psicológico, laboral, deportivo, etc.; ha permitido mayor desarrollo, ha llevado al mundo entero al ahorro de tiempos, distancias y mejoras en investigación, pero de igual forma, ha sido el punto de partida para que surjan nuevas modalidades de actos delincuenciales que se transforman a la par con la evolución de la tecnología, permitiendo que sean más rápidos, eficientes y con técnicas mejoradas.

Nacen palabras como cibercrimen, ciberdefensa, ciberterrorismo, ciberespacio y todas ellas enmarcadas dentro de la seguridad informática. En algunos países, el crimen informático es conocido como delincuencia informática, en otros, solo como ciberdelincuencia.

Desde sus inicios, las naciones más desarrolladas han tratado de luchar contra esta modalidad, utilizando todo lo que tienen a su alcance; las cifras por cibercrimen son muy altas, por esta razón después de muchos intentos, el consejo de Europa logró sacar avante la única ley de carácter internacional que se conocía hasta el momento, el convenio sobre ciberdelincuencia de Budapest, firmado en el año 2001 y que brinda la posibilidad a otros países no miembros del consejo de Europa, de adherirse al convenio y así poder luchar conjuntamente contra el flagelo de la delincuencia informática.

En los países de todo el mundo, se han presentado actos de delincuencia informática y de una forma u otra, algunos de ellos han tratado de establecer leyes para castigar muchos de estos delitos; sin embargo, la legislación aún es muy débil en la mayoría. Colombia por su parte, ha logrado realizar avances, y en el año 2011 fue invitada a ser parte del convenio de ciberdelincuencia de Budapest (a la adhesión solo se llega por invitación).

Siempre habrá personas que estarán interesadas en conocer, los efectos negativos o positivos que implica para los países no desarrollados, pertenecer a este tipo de convenios, y por supuesto también estará palpable el hecho de qué es lo que se necesita realmente en materia legal y de infraestructura para ser realmente un país adherido; sin embargo, la documentación al respecto no es suficiente y muchas veces deja un vacío de conocimiento muy grande.

2.1 ANTECEDENTES

La gran mayoría de los documentos encontrados por internet o en bibliotecas, son de carácter especializado, es decir, dedicados a un tema específico: legislación, social o gubernamental, no existe documentación de carácter integral que ayude a

comprender las ventajas y desventajas de la adhesión de Colombia o de cualquier otro país, a dicho convenio y desde diversos puntos de vista.

La información ubicada es específica y detallada, sin embargo, su panorama es limitado en cuanto al plano social, económico, cultural, legislativo e histórico de las diferentes naciones que pueden o no pensar en adherirse al Convenio de Ciberdelincuencia de Budapest.

2.2 MARCO TEORICO

En torno al tema de la seguridad informática, son muchos los conceptos que revisten gran importancia, razón por la cual para la investigación, se tomaron los más relevantes en línea directa al estudio realizado.

2.2.1 Reseña histórica

Desde los inicios de la humanidad el hombre siempre ha tenido la necesidad de comunicarse con sus congéneres, en unos comienzos lo realizaron a través de señales, humo, pictográficamente, lenguaje y tantos otros; sin embargo, la evolución ha llevado a la raza humana a alcanzar un gran nivel en lo referente a esto, es así, como a través de las diferentes épocas, el hombre busco nuevas formas de manejar, controlar, custodiar y procesar la información que a través de la comunicación termino convirtiéndose en el activo más importante de la actual era.

La aparición de Internet, que fuese en un principio una herramienta de carácter militar en los años 60 y que posteriormente daría origen a lo que se conociera como ARPANET. A “ARPANET, posibilitó la conexión de muchas universidades que colaboraron en el tema de defensa. De ahí, surgió la necesidad de conectar ordenadores de diferentes clases, por lo que, en 1983, se implanto el protocolo TCP/IP permitiendo conectar cualquier computador”.[1]

Para finales de la década de los 80, ya todo el mundo estaría conectado por medio de internet, década tras década se ha convertido en la forma más idónea para manipular la información; así, el rápido crecimiento tecnológico llevo a que muchas personas tuviesen acceso a computadores de escritorio, computadores portátiles, luego tabletas y ahora teléfonos móviles inteligentes.

El aumento de tecnología y reducción de costos permitió que mucha gente accediera a todo tipo de dispositivos con los cuales podría almacenar, transferir,

[1] AZNAR, A. La red Internet. El modelo TCP/IP. Madrid: 2005 Grupo Abantos formación y consultoría. Pág. 61

enviar y manipular su información a gran velocidad y con mucha facilidad. Si bien no fue posible ver las dimensiones que llegaría a tener internet, tampoco fue posible prever la cantidad de delitos de carácter informático que se presentarían y que día a día aumentan.

Con el desmesurado crecimiento de la tecnología y la reducción de los costos de los computadores, teléfonos móviles y dispositivos electrónicos, la sociedad comenzó un proceso de hiperconectividad de dimensiones no concebidas; pese a ello, la mayoría de los usuarios de esta tecnología, no tiene la suficiente capacitación para proteger su información de los delincuentes informáticos.

En las gráficas y tablas siguientes, se presenta un estudio realizado por La UIT, organismo especializado de las Naciones Unidas para las tecnologías de la información y la comunicación – TIC, en el cual se podrán encontrar estadísticas de los últimos 14 años en los cuales se muestra una breve radiografía de la expansión de internet y el uso de la telefonía móvil alrededor del mundo, lo cual evidencia un leve panorama del nivel de riesgo al que se está expuesto constantemente. Los datos se han clasificado en países desarrollados, países en desarrollo y a nivel mundial; para el año 2016 el dato aparece estimado.

Como se puede ver, en cuanto a tener internet en el hogar, un país desarrollado paso de tener un porcentaje de 35% en el año 2002 a 81,3% en el año 2015, y un país en desarrollo de 4,6% a 41,1%, cifras que evidencian claramente el crecimiento de internet en los hogares de todo el mundo.

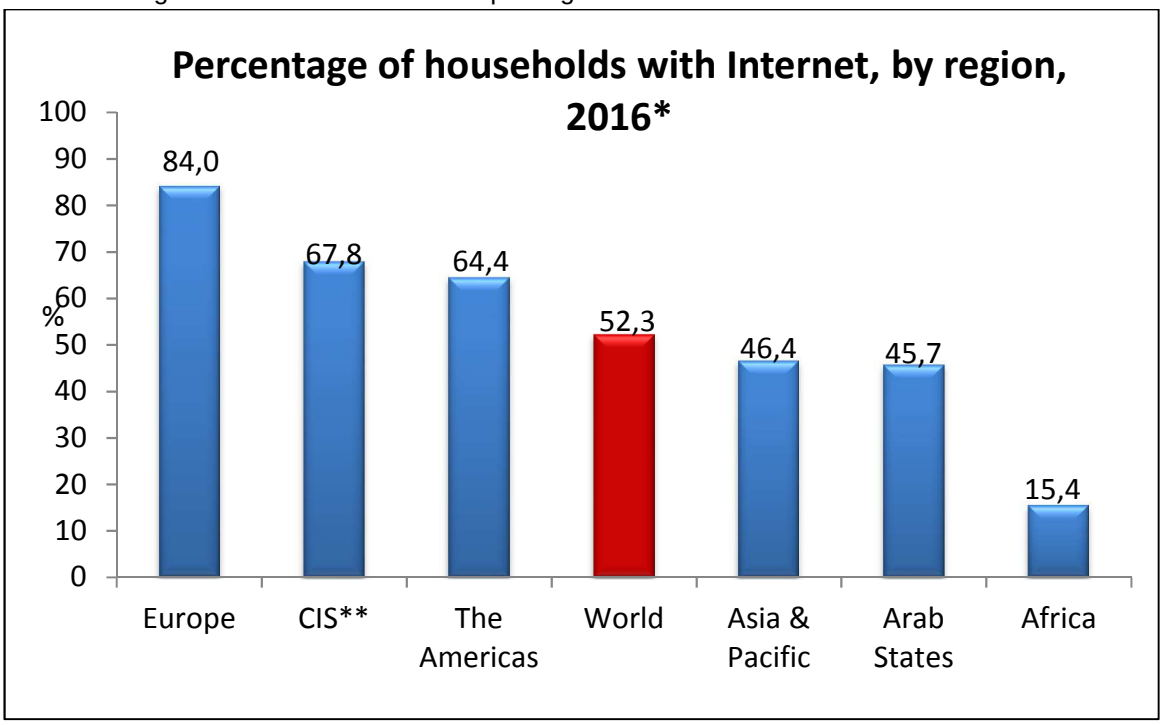
Tabla 1 Hogares con acceso a Internet

	Porcentaje de hogares con acceso a internet														
Año	**2002**	**2003**	**2004**	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016***
Desarrollado	35,0	38,8	41,4	44,7	48,2	53,4	57,7	62,6	66,2	69,2	73,1	77,4	79,5	81,3	83,8
Mundial	13,4	15,3	16,9	18,4	20,5	23,0	24,8	27,0	30,0	33,4	37,9	41,8	45,1	49,0	52,3
En Desarrollo	4,6	5,8	7,0	8,1	9,6	11,2	12,3	13,6	16,6	20,2	25,0	28,9	32,9	37,6	41,1

Fuente 1 The developed/developing country classifications are based on the UN M49,

Se estimaba que para el año 2016 el porcentaje de viviendas con acceso a internet sea el evidenciado en el siguiente gráfico:

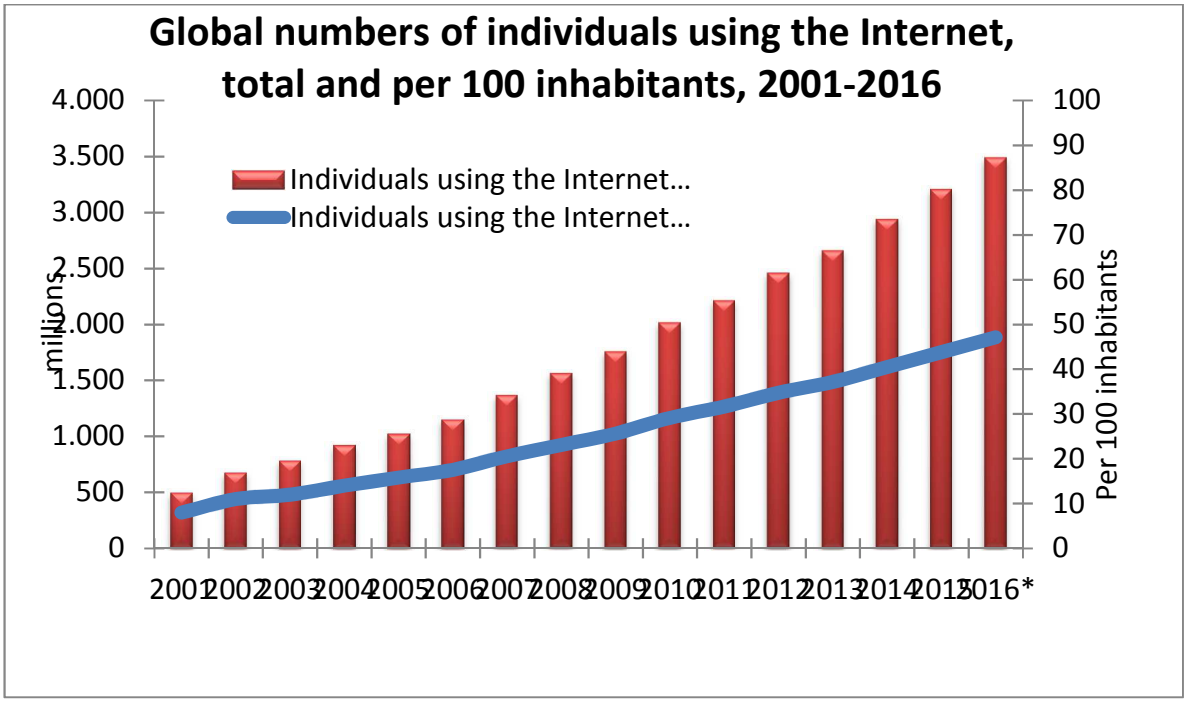
Grafica 1 Hogares con acceso a Internet por región



Fuente 2 ITU World Telecommunication/ICT Indicators database, Regions are based on the ITU BDT Regions, Disponible en: http://www.itu.int/en/ITU-D/Statistics/Pages/definitions/regions.aspx

Pero el uso de internet en el mundo es aún más aterrador, en el 2001 solo 495 millones de personas lo utilizaban, el año 2015 se registró una cantidad de 3.207 millones de personas, equivalente a un incremento de casi 8 veces en 15 años y se estimaba que para el año 2016 fuese de 3.488 millones de personas.

Grafica 2 Individuos que usan Internet



Fuente 3 ITU World Telecommunication/ICT Indicators database, Disponible en: http://www.itu.int/en/ITU-D/Statistics/Pages/definitions/regions.aspx

La tecnología móvil ha presentado una dinámica más fuerte, los países en desarrollo de tener 250 millones de personas suscritas en el año 2000 pasaron a un estimado 5.777 millones de personas suscritas para el 2016, lo cual demuestra que muchas personas hoy en día tienen acceso a información de forma inmediata, esto es, un crecimiento de 23 veces en 16 años.

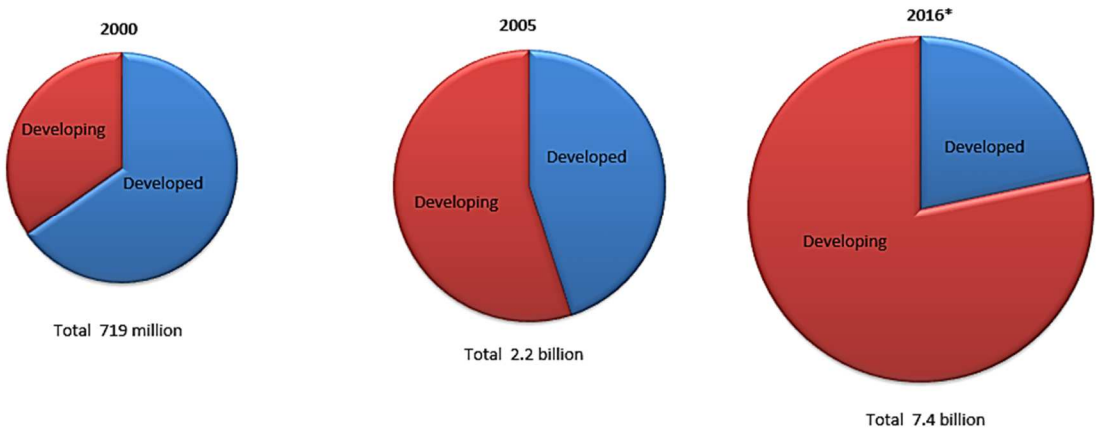
Tabla 2 Suscripción a telefonía móvil

Año	**2000**		**2005**		**2016***	
Suscripción a telefonía móvil (en millones)	**Desarrollado**	**En Desarrollo**	**Desarrollado**	**En Desarrollo**	**Desarrollado**	**En Desarrollo**
	469	250	992	1.213	1.600	5.777
Total	719		2.205		7.377	

Fuente 4 ITU World Telecommunication/ICT Indicators database. The developed/developing country classifications are based on the UN M49, Disponible en: http://www.itu.int/en/ITU-D/Statistics/Pages/definitions/regions.aspx.html

La suscripción en telefonía móvil paso de 719 millones en el año 2000 a 7.4 billones estimados para el 2016.

Grafica 3 Suscripción a telefonía móvil



Fuente 5 ITU World Telecommunication/ICT Indicators database. The developed/developing country classifications are based on the UN M49, Disponible en: http://www.itu.int/en/ITU-D/Statistics/Pages/definitions/regions.aspx.html

Como era de suponer y claramente se hizo realidad, entre más aumentaba la cobertura y el uso de internet también lo hizo la delincuencia informática. La primera necesidad de atentar contra los sistemas informáticos tal vez fue el reconocimiento, pero esta fue evolucionando y aparecieron otros intereses como la diversión, los factores económicos, ideología, un afán de autorrealización con reconocimiento social; aunque hoy en día perduran todas, la más notoria es la de una retribución económica. Las maneras de atacar han evolucionado con el transcurrir del tiempo, pero en esencia son de la misma forma, ataques pasivos o activos, entre los cuales se pueden encontrar:

- ✓ Actividades de reconocimiento de sistemas, cuyo único ideal es recoger información de las víctimas potenciales.
- ✓ Encontrar vulnerabilidades en los sistemas, por lo general apoyados por medio del uso de Exploits.
- ✓ Interceptación de mensajes y robo de la información permitiendo obtener datos de carácter valioso.
- ✓ Análisis de tráfico a través de las redes, en este caso se pueden valer de Sniffers.

- ✓ Suplantación de identidad, mediante el cual pueden llegar a obtener claves, usuarios y otros, acá utilizan técnicas como IP Spoofing, DNS Spoofing, modificación de registros de Dominios, SMTP Spoofing, uso de software espía.
- ✓ Conexiones no autorizadas a los equipos de la organización, la cual se puede dar por puertas traseras, rootkits o wardialing.
- ✓ Virus informáticos como troyanos o gusanos.
- ✓ Ataques por medio de código script XSS Cross Site Scripting
- ✓ Inyección SQL mediante el cual atacan bases de datos
- ✓ Ataques criptográficos como el Ramsonware, Clickjacking
- ✓ Denegación de servicio por medio del cual se colapsa un sitio.

Hoy en día con la expansión de internet no es imprudente asegurar que cualquier persona en cualquier parte del mundo está expuesta a ser atacada desde cualquier país y en cualquier momento.

2.2.2 Historia de la Legislación y Seguridad Informática. Con el desarrollo de internet también creció la tecnología y en gran medida la delincuencia informática, a la cual de acá en adelante denominaremos como “cibercrimen”, por esta razón es que desde los años 80 se realizaron intentos de volver la red un poco más segura.

En 1986, se promulga la Ley de Privacidad de Comunicaciones Electrónicas, aprobada para ordenar restricciones en el uso de los ordenadores, era la primera vez que un gobierno (EEUU) trataba de contener a Internet[2]; no obstante, esta ley resulto de difícil aplicación en algunos casos, y quedo al descubierto como la delincuencia en internet se extendía fuera de los límites de Estados Unidos a continentes enteros como Europa. A continuación, veremos algunos ejemplos del documento “Cómo manejan los países el delito informático” que escribió Michael Kim al Instituto Tecnológico de Massachusetts (MIT), en el año 1997:

En el Reino Unido Woods y Strickland, más conocido como Pad y Gandalf realizan ataques en 15 países diferentes, derribando parte de la red telefónica de Suecia, robando registros financieros del principal banquero de Londres y exponer cuentas de gastos del presidente de la Comunidad Europea, se les condena solo por el mal uso de computadoras[3]. Para este año el país solo contaba con la ley de abusos informáticos de 1990 y la Ley de Protección de Datos de 1984.

---

[2]KIM, Michael. ¿Cómo manejan los países los delitos informáticos? [Online]. Estados Unidos: 1997. [citado 2016-11-20]. Disponible en internet <http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall97-papers/kim-crime.html>.

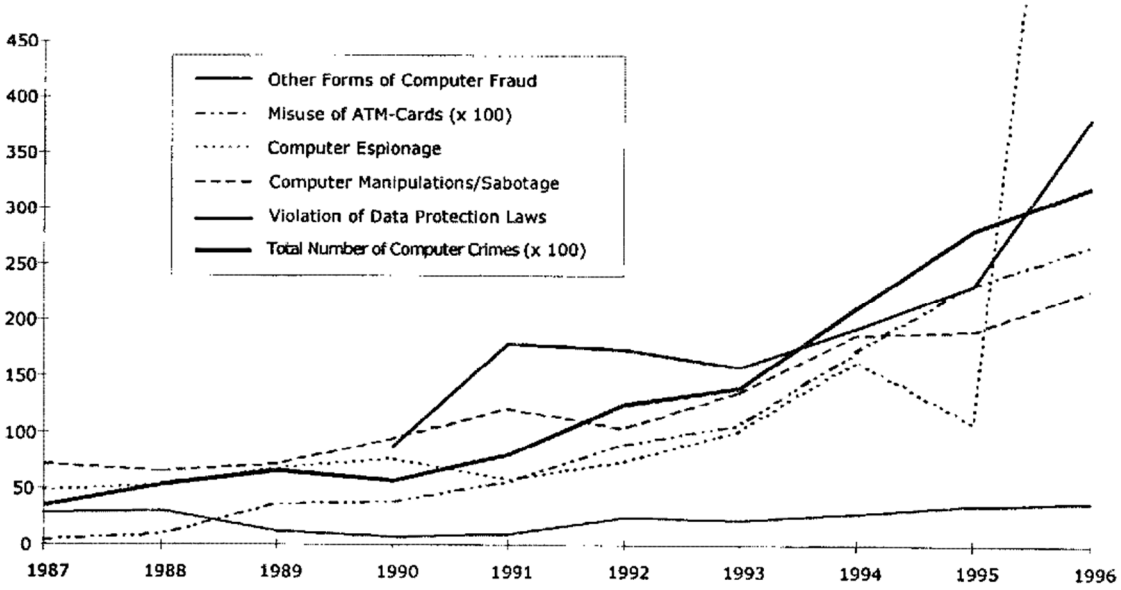
[3] KIM. Op. Cit. Disponible en internet <http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall97-papers/kim-crime.html>.

Italia en 1994, lanza una operación conocida como Hardware1 para combatir la piratería a nivel nacional, y en la cual se vio involucrada la BBS (Bits Against the Empire), pero toda la operación se vio opacada por corrupción del Estado; también descubrieron a finales del año, un virus en los servidores italianos de origen búlgaro, pero, no se presentaron cargos.[4]

En Dinamarca JubJub y Piñón, dos chicos de escuela secundaria, fueron descubiertos al husmear en la NASA. Se les dio una sentencia de dos años de libertad condicional, durante los cuales se les prohibió expresamente tocar cualquier equipo[5]. En este caso se presentaron muchos problemas para poder juzgar a los chicos en vista de que no existían un tratado entre Dinamarca y Estados Unidos sobre el tema que permitiera emitir una condena, fue un caso bastante demorado.

El panorama por parte de Alemania era muy similar, en el documento, Aspectos Legales de la Delincuencia Informática en la Sociedad de la Información, preparado por el DR. Ulrich Sieber de la Universidad de Würzburg, a comienzos del año 1998, presentado para la Comisión Europea se evidencia:

Figura 1 Número de delitos informáticos informados a la policía alemana



Fuente 6 http://www.oas.org/juridico/english/COMCRIME%20Study.pdf

[4] KIM. Op. Cit. Disponible en internet <http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall97-papers/kim-crime.html>.

[5] KIM. Op. Cit. Disponible en internet <http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall97-papers/kim-crime.html>.

En la figura 1 se muestra un crecimiento muy fuerte en los delitos de carácter informático; claro que la radiografía no se presenta solo en Europa y Estados Unidos, a finales del año 2000 se presenta un reporte por parte de McConnell International, denominado “¿Delincuencia en el ciberespacio…. y el castigo? Las Leyes Arcaicas Amenaza Mundial a la Información” donde se muestra una sencilla y evidente radiografía a nivel mundial, de la problemática presentada en cuanto a legislación.

Tabla 3 Países con leyes sobre seguridad informática al 2000

Country	Data Crimes			Network Crimes		Access Crimes		Related Crimes		
	Data Interception	Data Modification	Data Theft	Network Interference	Network Sabotage	Unauthorized Access	Virus Dissemination	Aiding and Abetting Cyber Crimes	Computer-Related Forgery	Computer-Related Fraud
Australia	✔	✔	✔	✔		✔			✔	✔
Brazil		✔			✔	✔		✔		
Canada	✔	✔	✔	✔	✔	✔	✔			✔
Chile	✔	✔	✔	✔	✔					
China		✔		✔			✔			
Czech Republic		✔	✔		✔	✔				✔
Denmark		✔		✔						✔
Estonia		✔	✔	✔	✔	✔	✔	✔		✔
India		✔	✔	✔	✔	✔	✔	✔		✔
Japan	✔	✔	✔	✔	✔	✔		✔	✔	✔
Malaysia		✔				✔		✔		✔
Mauritius	✔	✔		✔	✔	✔	✔	✔	✔	
Peru	✔	✔	✔	✔	✔	✔				✔
Philippines	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Poland		✔	✔	✔				✔		
Spain	✔	✔	✔					✔		✔
Turkey		✔	✔	✔	✔		✔	✔	✔	✔
United Kingdom		✔		✔	✔	✔		✔		
United States	✔	✔	✔	✔	✔	✔	✔	✔		✔

Fuente 7 http://www.iwar.org.uk/law/resources/cybercrime/mcconnell/CyberCrime.pdf

- "Data Interception: Interceptación de datos en la transmisión.
- Data Modification: La alteración, destrucción o eliminación de los datos.
- Data Theft: Tomar o copiar datos, independientemente de si se encuentra protegido por otras leyes, por ejemplo, los derechos de autor, privacidad, etc.

- Network Interference: que dificultan o impiden el acceso a los demás. El ejemplo más común de esta acción está instigando una denegación de servicio distribuido ataque (DDoS), los sitios Web de inundación o Proveedores de Servicios de Internet. ataques DDoS a menudo se lanzan desde numerosos ordenadores que han sido manipulados para obedecer órdenes del perpetrador.
- Network Sabotage: La modificación o destrucción de una red o sistema.
- Unauthorized Access: pirateo informático para obtener acceso a un sistema o datos.
- Virus Dissemination: Introducción de software de dañar a los sistemas o datos.
- Aiding and Abetting: Habilitación de la comisión de un delito informático.
- Computer-Related Forgery: Alteración de datos con la intención de representar lo más auténtico.
- Computer-Related Fraud: La alteración de los datos con la intención de sacar partido económico de su falsedad".[6]

A pesar de contar con legislación, muchos de los países relacionados en el cuadro anterior, no la aplican correctamente o simplemente se colocaba en práctica de diferente forma en sus Estados o Departamentos. A veces tenían cambios acordes a la connotación de los agresores, edades u otros, las leyes tendían a ser permisivas o ambiguas.

Tanto Estados Unidos como Europa comenzaron a realizar intentos para contrarrestar los delitos informáticos, prácticamente desde su comienzo, pero es Europa, a través del Consejo de Europa, que logra el primer y único convenio en su género denominado, Convenio de Ciberdelincuencia de Budapest, en el año 2001.

Se puede afirmar claramente que desde noviembre de 1996 por medio de la expedición de la resolución CDPC / 103211196, el Comité Europeo de Problemas Penales tomo la decisión de reunir expertos para trabajar en el tema y hacerle frente al ciberdelito.[7]

Es de aclarar, que este convenio requirió de casi 30 versiones, cuatro años de trabajo y numerosas críticas, al igual que el apoyo de algunos países que estaban como observadores (evidenciable en la figura 2), pero las cifras en cibercriminal eran alarmantes, “fraudes con tarjetas de crédito reportaron 400 millones de dólares

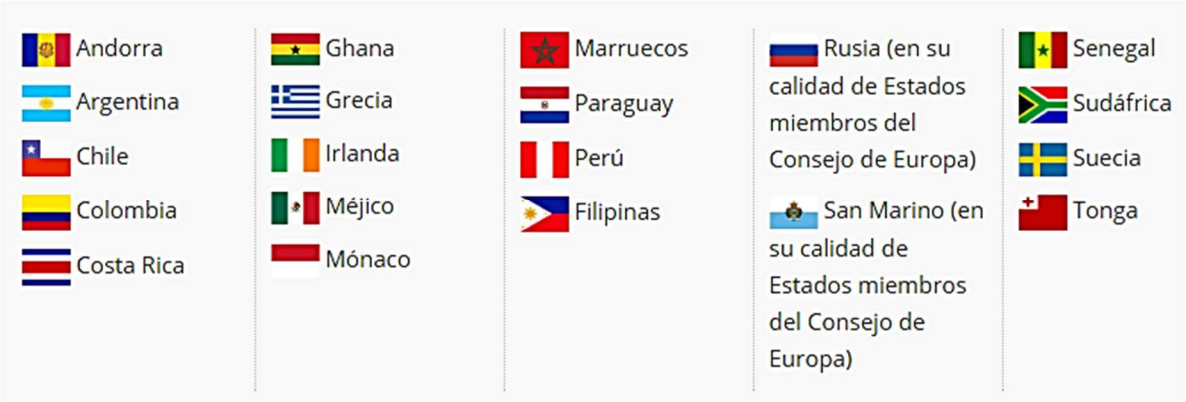
---

[6] INTERNATIONAL MCCONNELL. Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information. [Online]. Washington DC: 2011. [citado 2016-11-20]. Disponible en internet: <http://www.iwar.org.uk/law/resources/cybercrime/mcconnell/CyberCrime.pdf>

[7] EUROPE. Council of. Explanatory Report to the Convention on Cybercrime, European Treaty Series - No. 185. [Online]. Budapest: 2001. [citado 2016-11-20]. Disponible en internet <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b>.

en 1999, gastos derivados de la acción de virus informáticos costaron cerca de 12.000 millones de dólares, empresas víctimas de la piratería o la imitación de obras dejan de ganar unos 250.000 millones de dólares por año, según el Consejo, la pornografía infantil, los informes de UNICEF señalan que, tan sólo en Estados Unidos, genera entre 2.000 y 3.000 millones de dólares"[8]

Figura 2 Países observadores



Fuente 8 http://www.coe.int/en/web/cybercrime/parties-observers

En un comienzo (como se puede ver en la figura 3) los países firmantes miembros fueron Albania, Armenia, Austria, Bélgica, Bulgaria, Croacia, Chipre, Estonia, Finlandia, Francia, Alemania, Grecia, Hungría, Islandia, Italia, Moldavia, Países Bajos, Noruega, Polonia, Portugal, Rumania, España, Suecia, Suiza, La ex República Yugoslava de Macedonia, Ucrania, Reino Unido y los países no miembros que se adhirieron fueron Canadá, Japón, Estados Unidos y Sudáfrica

[8] PREES, Europa. España se suma a la propuesta, Treinta países firman la primera Convención Internacional contra el 'Cibercrimen'. [Online]. España: 2001. [citado 2016-11-20]. Disponible en internet <http://www.elmundo.es/navegante/2001/11/26/esociedad/1006766268.html>.

Figura 3 Miembros del convenio de ciberdelincuencia a octubre 16 de 2016

Fuente 9 http://www.coe.int/en/web/cybercrime/parties-observers

Las organizaciones observadoras fueron:

- ✓ Comisión de la Unión Africana (AUC)
- ✓ Secretaría del Commonwealth
- ✓ Unión Europea (Comisión Europea y el Consejo de la Unión Europea, Eurojust, Europol, la Red Europea y la Agencia de Seguridad de la Información (ENISA))
- ✓ G8 delincuencia de alta tecnología Subgrupo
- ✓ Unión Internacional de Telecomunicaciones (UIT)
- ✓ Interpol
- ✓ Organización para la Cooperación y el Desarrollo Económico (OCDE)
- ✓ Organización para la Seguridad y la Cooperación en Europa (OSCE)
- ✓ Organización de los Estados Americanos (OEA)
- ✓ Oficina de las Naciones Unidas contra la Droga y el Delito (ONUDD).[9]

En el marco teórico es indispensable tener presente documentos de alto contenido para la investigación los cuales se presentan en su totalidad y respetando su formato de publicación, entre ellos están el Convenio de Ciberdelincuencia de Budapest, Ley 1273 de 2009, Ley 1336 de 2009, Ley Estatutaria 1266 DE 20081 y

[9] PORTAL, Council of Europe. Parties/Observers to the Budapest Convention and Observer Organizations to the T-CY. [Online]. Council of Europe: 2017. [citado 2016-11-20]. Disponible en internet <http://www.coe.int/en/web/cybercrime/parties-observers>.

la Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información en Colombia

2.2.3 Convenio de Ciberdelincuencia de Budapest. Se puede decir a ciencia cierta que, hasta el día de hoy, es el único convenio de carácter internacional que apoyado en la normatividad legal y penal, busca combatir los delitos de carácter informático a nivel mundial; se originó en el Consejo de Europa y es una buena guía para que los demás países del mundo puedan adoptar medidas legislativas que puedan ayudar a luchar contra el cibercrimen y ciberterrorismo.

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 nº 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, nº R (88) 2 sobre medidas encaminadas a luchar contra la piratería en materia de propiedad intelectual y derechos afines, nº R (87) 15 relativa a la regulación de la utilización de datos personales por la policía, nº 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 nº 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 nº R (95) 13 relativa a las cuestiones de procedimiento penal vinculadas a la tecnología de la información;

Teniendo en cuenta la Resolución nº 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 nº 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:
Toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar por medio de un sistema informático, y 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 entender· 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 entender· toda persona menor de 18 años. No obstante, cualquier Parte podrá· establecer un límite de edad inferior, que ser· como mínimo de 16 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 adoptar 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 los 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 transmite 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 15.

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 ilícitamente 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 o 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 nº 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 garantizarà 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 comunicar· 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 indicar·:
   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 transmite 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 ilícito 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.

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 nº 24);
   – el Convenio europeo de asistencia judicial en materia penal, abierto a la firma en Estrasburgo el 20 de abril de 1959 (STE nº 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 nº 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 examinar· 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.

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 surtir· 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 notificar· 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 relativa 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 depositar· en los archivos del Consejo de Europa. El Secretario General del Consejo de Europa remitir· 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.

LA JEFE DE AREA DE LA OFICINA DE INTERPRETACION DE LENGUAS CERTIFICA: Que la precedente traducción está· fiel y literalmente hecha de un documento en francés e inglés que a tal efecto se me ha exhibido. Madrid, a 9 de enero de dos mil dos

2.2.4 Delito Informático. Es un término que nace en la década de los años 90 a raíz de los problemas que se presentaran en los Estados Unidos de Norteamérica por los delitos que se cometían a través de la red, se define como "acción u omisión realizada por un ser humano que cause perjuicio a personas sin que necesariamente se beneficie, o que, produzca un beneficio ilícito, aunque no perjudique directa o indirectamente a la víctima y que se realiza por medio informático"[10].

Los delitos informáticos son de muy variados tipos y su clasificación cambia de un país a otro (lo cual no es lógico, pero depende de la legislación y otras variables).

Dada la afinidad que comparte Colombia y España en algunos aspectos legales y culturales y por ser este último, un país europeo miembro del convenio de Budapest, se comenzará por relacionar los delitos clasificados como informáticos por la Brigada de Investigación Tecnológica de la Policía Nacional Española, a saber:

- ✓ "Ataques que se producen contra el derecho a la intimidad:
  Delito de descubrimiento y revelación de secretos mediante el apoderamiento y difusión de datos reservados registrados en ficheros o soportes informáticos. (Artículos del 197 al 201 del Código Penal)
- ✓ Infracciones a la Propiedad Intelectual a través de la protección de los derechos de autor:
  Especialmente la copia y distribución no autorizada de programas de ordenador y tenencia de medios para suprimir los dispositivos utilizados para proteger dichos programas. (Artículos 270 y otros del Código Penal)
- ✓ Falsedades:
  Concepto de documento como todo soporte material que exprese o incorpore datos. Extensión de la falsificación de moneda a las tarjetas de débito y crédito. Fabricación o tenencia de programas de ordenador para la comisión de delitos de falsedad. (Artículos 386 y ss. del Código Penal)
- ✓ Sabotajes informáticos:
  Delito de daños mediante la destrucción o alteración de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos. (Artículo 263 y otros del Código Penal)
- ✓ Fraudes informáticos:

[10] FLOREZ, Lucerito. Derecho informático. México: Grupo editorial patria. 2014. Pág. 24

Delitos de estafa a través de la manipulación de datos o programas para la obtención de un lucro ilícito. (Artículos 248 y ss. del Código Penal)

- ✓ Amenazas:

Realizadas por cualquier medio de comunicación. (Artículos 169 y ss. del Código Penal)

- ✓ Calumnias e injurias:

Cuando se propaguen por cualquier medio de eficacia semejante a la imprenta o la radiodifusión. (Artículos 205 y ss. del Código Penal)

- ✓ Pornografía infantil:

Entre los delitos relativos a la prostitución al utilizar a menores o incapaces con fines exhibicionistas o pornográficos.

La inducción, promoción, favorecimiento o facilitamiento de la prostitución de una persona menor de edad o incapaz. (Art 187)

La producción, venta, distribución, exhibición, por cualquier medio, de material pornográfico en cuya elaboración hayan sido utilizados menores de edad o incapaces, aunque el material tuviere su origen en el extranjero o fuere desconocido. (Art 189)

El facilitamiento de las conductas anteriores (El que facilitare la producción, venta, distribución, exhibición...). (Art 189)

La posesión de dicho material para la realización de dichas conductas. (Art 189)".[11]

2.2.5 Ley 1273 de 2009

(Enero 05)

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

EL CONGRESO DE COLOMBIA

DECRETA:

Artículo 1°. Adiciónase el Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos", del siguiente tenor:

[11] BRIGADA DE INVESTIGACIÓN TECNOLÓGICA, Policía Española. [Online]. España: 2015. [citado 2016-12-20]. Disponible en internet <http://delitosinformaticos.info/delitos_informaticos/tipos_delitos.html>.

CAPITULO. I

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

Artículo 269A: *Acceso abusivo a un sistema informático*. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269B: *Obstaculización ilegítima de sistema informático o red de telecomunicación.* El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: *Interceptación de datos informáticos*. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: *Daño Informático*. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E: *Uso de software malicioso*. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: *Violación de datos personales*. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda,

intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G: *Suplantación de sitios web para capturar datos personales*. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269H: *Circunstancias de agravación punitiva*: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

2. Por servidor público en ejercicio de sus funciones.

3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

5. Obteniendo provecho para sí o para un tercero.

6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

7. Utilizando como instrumento a un tercero de buena fe.

8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

CAPITULO. II

De los atentados informáticos y otras infracciones

Artículo 269I: *Hurto por medios informáticos y semejantes*. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Artículo 269J: *Transferencia no consentida de activos*. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

Artículo 2°. Adiciónese al artículo 58 del Código Penal con un numeral 17, así:

Artículo 58. *Circunstancias de mayor punibilidad*. Son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera:

(...)

17. Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos.

Artículo 3°. Adiciónese al artículo 37 del Código de Procedimiento Penal con un numeral 6, así:

Artículo 37. *De los Jueces Municipales*. Los jueces penales municipales conocen:

(...)

6. De los delitos contenidos en el título VII Bis.

Artículo 4°. La presente ley rige a partir de su promulgación y deroga todas las disposiciones que le sean contrarias, en especial el texto del artículo 195 del Código Penal.

El Presidente del honorable Senado de la República,

Hernán Andrade Serrano.

El Secretario General del honorable Senado de la República,

Emilio Ramón Otero Dajud.

El Presidente de la honorable Cámara de Representantes,

Germán Varón Cotrino.

El Secretario General de la honorable Cámara de Representantes,

Jesús Alfonso Rodríguez Camargo.

REPUBLICA DE COLOMBIA - GOBIERNO NACIONAL

Publíquese y cúmplase.

Dada en Bogotá, D. C., a 5 de enero de 2009.

ÁLVARO URIBE VÉLEZ

El Ministro del Interior y de Justicia,

Fabio Valencia Cossio.

NOTA: Publicada en el Diario Oficial 47.223 de enero 5 de 2009.

2.2.6 Ley 1336 de 2009

(Julio 21)

Por medio de la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes.

El Congreso de Colombia

DECRETA:

Artículo 1°. *Autorregulación en servicios turísticos y en servicios de hospedaje turístico*. Los prestadores de servicios turísticos y los establecimientos que presten el servicio de hospedaje no turístico deberán adoptar, fijar en lugar público y

actualizar cuando se les requiera, códigos de conducta eficaces, que promuevan políticas de prevención y eviten la utilización y explotación sexual de niños, niñas y adolescentes en su actividad, los cuales serán diseñados de conformidad con lo previsto en el inciso 2° del presente artículo.

Un modelo de estos códigos se elaborará con la participación de organismos representativos de los sectores. Para estos efectos, el Ministerio de Comercio, Industria y Turismo respecto a los prestadores de servicios turísticos y la Superintendencia de Industria y Comercio respecto a los establecimientos de alojamiento no turístico, convocarán a los interesados. Tales códigos serán adoptados dentro del año siguiente a la vigencia de la presente ley, y serán actualizados en función de nuevas leyes, nuevas políticas o nuevos estándares de protección de la niñez adoptados en el seno de organismos internacionales, gubernamentales o no.

El Ministerio de Comercio, Industria y Turismo y la Superintendencia de Industria y Comercio adoptarán medidas administrativas tendientes a verificar el cumplimiento tanto de la adopción como de la actualización y cumplimiento constante de los códigos. Para tales efectos podrá solicitar a los destinatarios de esta norma la información que se considere necesaria. El Ministerio de Comercio, Industria y Turismo y la Superintendencia de Industria y Comercio ejercerán las funciones de verificación de las obligaciones contempladas en este inciso y de sanción por causa de su omisión, conforme a lo dispuesto en el artículo 20 de la Ley 679 de 2001.

Las autoridades distritales y municipales realizarán actividades periódicas de inspección y vigilancia de lo dispuesto en este artículo, en caso de encontrar incumplimiento deberán remitir la información al Ministerio de Comercio, Industria y Turismo y la Superintendencia de Industria y Comercio, según el caso.

Artículo 2°. *Autorregulación de aerolíneas.* Las aerolíneas adoptarán códigos de conducta eficaces que promuevan políticas de prevención y eviten la utilización y explotación sexual de niños, niñas y adolescentes en su actividad.

Un modelo de estos sistemas y códigos se elaborará con la participación de organismos representativos del sector. Para estos efectos, la Aeronáutica Civil convocará a los interesados a que formulen por escrito sus propuestas de códigos de conducta. Tales códigos serán adoptados dentro del año siguiente a la vigencia de la presente ley, copia de los cuales se remitirá a la oficina que indique la Aeronáutica y serán actualizados cada vez que se considere necesario en función de nuevas leyes, nuevas políticas o nuevos estándares de protección de la niñez adoptados en el seno de organismos internacionales, gubernamentales o no.

La Aeronáutica adoptará, medidas administrativas tendientes a verificar el cumplimiento tanto de la adopción como de la actualización y cumplimiento constante de los códigos. Para este último efecto podrá solicitar a los destinatarios de esta norma la información que considere necesaria.

El incumplimiento de esta norma por las autoridades genera las consecuencias disciplinarias de rigor. El incumplimiento de esta norma por parte de aerolíneas genera las consecuencias administrativas sancionatorias aplicables al caso de violación a las instrucciones administrativas del sector.

Artículo 3°. *Competencia para exigir información.* El artículo 10 de la Ley 679 de 2001 tendrá un parágrafo del siguiente tenor:

"**Parágrafo.** El Ministerio de Comunicaciones tendrá competencia para exigir, en el plazo que este determine, toda la información que considere necesaria a los proveedores de servicios de internet, relacionada con la aplicación de la Ley 679 y demás que la adicionen o modifiquen. En particular podrá:

1. Requerir a los proveedores de servicios de internet a fin de que informen en el plazo y forma que se les indique, qué mecanismos o filtros de control están utilizando para el bloqueo de páginas con contenido de pornografía con menores de edad en Internet.

2. Ordenar a los proveedores de servicios de internet incorporar cláusulas obligatorias en los contratos de portales de internet relativas a la prohibición y bloqueo consiguiente de páginas con contenido de pornografía con menores de edad.

Los proveedores de servicios de internet otorgarán acceso a sus redes a las autoridades judiciales y de policía cuando se adelante el seguimiento a un número IP desde el cual se produzcan violaciones a la presente ley.

La violación de estas disposiciones acarreará la aplicación de las sanciones administrativas de que trata el artículo 10 de la Ley 679 de 2001, con los criterios y formalidades allí previstas.

Artículo 4°. *Autorregulación de café Internet.* Todo establecimiento abierto al público que preste servicios de Internet o de café Internet deberá colocar en lugar visible un reglamento de uso público adecuado de la red, cuya violación genere la suspensión del servicio al usuario o visitante.

Ese reglamento, que se actualizará cuando se le requiera, incluirá un sistema de autorregulación y códigos de conducta eficaces que promuevan políticas de prevención de explotación sexual de niños, niñas y adolescentes, y que permitan proteger a los menores de edad de toda forma de acceso, consulta, visualización o exhibición de pornografía.

Un modelo de estos sistemas y códigos se elaborará con la participación de organismos representativos del sector. Para estos efectos, el Ministerio de Comunicaciones convocará a los interesados a que formulen por escrito sus propuestas de autorregulación y códigos de conducta. Tales códigos serán adoptados dentro del año siguiente a la vigencia de la presente ley, copia de los

cuales se remitirá a la oficina que indique el Ministerio de Comunicaciones, de su propia estructura o por delegación a los municipios y distritos, y serán actualizados cada vez que el Ministerio de Comunicaciones lo considere necesario en función de nuevas leyes, nuevas políticas o nuevos estándares de protección de la niñez adoptados en el seno de organismos internacionales, gubernamentales o no.

Las autoridades distritales y municipales realizarán actividades periódicas de inspección y vigilancia de lo dispuesto en este artículo y sancionarán su incumplimiento de conformidad con los procedimientos contenidos en el Código Nacional de Policía y los códigos departamentales y distritales de policía que apliquen.

El incumplimiento de los deberes a que alude esta norma dará lugar a las mismas sanciones aplicables al caso de venta de licor a menores de edad.

Artículo 5°. *Adhesión a los códigos de conducta por parte de los prestadores de servicios turísticos.* El Ministerio de Comercio, Industria y Turismo, exigirá a los prestadores de servicios turísticos para efectos de su inscripción en el Registro Nacional de Turismo su adhesión al código de conducta señalado en el artículo 1° de esta ley. Igualmente requerirá a los prestadores de servicios turísticos ya inscritos a fin de que en los plazos y condiciones establecidos para la primera actualización del Registro que se efectúe con posterioridad a la elaboración de los códigos de conducta de que trata el artículo 1°, adhieran a los mismos. De la misma manera se procederá cada vez que los códigos de conducta sean modificados de acuerdo con lo dispuesto en el artículo 1°, solicitando su adhesión ya sea en la inscripción de los nuevos prestadores o bien en la siguiente actualización del Registro Nacional de Turismo a los prestadores ya inscritos. La no adhesión a los códigos de conducta por parte de los prestadores impedirá que el Ministerio realice la correspondiente inscripción o actualización.

Artículo 6°. *Estrategias de sensibilización.* El Ministerio de Comercio, Industria y Turismo adelantará estrategias de sensibilización e información sobre el fenómeno del turismo sexual con niños, niñas y adolescentes, y solicitará para el efecto el concurso no sólo de los prestadores de servicios turísticos, sino también de los sectores comerciales asociados al turismo. El ICBF se integrará a las actividades a que se refiere este artículo, a fin de asegurar la articulación de tales estrategias con el Plan Nacional para la Erradicación de la Explotación Sexual Comercial de Niños, Niñas y Adolescentes.

Artículo 7°. *Promoción de las estrategias.* Los prestadores de servicios turísticos, aerolíneas y empresas de servicio de transporte intermunicipal, prestarán su concurso a fin de contribuir con la difusión de estrategias de prevención de la explotación sexual de niños, niñas y adolescentes en actividades ligadas al turismo, utilizando para ello los programas de promoción de sus planes turísticos y medios de comunicación de que dispongan, cuando sean requeridos para el efecto por el

Ministerio de Comercio, Industria y Turismo o el Instituto Colombiano de Bienestar Familiar.

Artículo 8°. *Aviso Persuasivo.* Sin excepción, todo establecimiento donde se venda o alquile material escrito, fotográfico o audiovisual deberá fijar en lugar visible un aviso de vigencia anual que llevará una leyenda preventiva acerca de la existencia de legislación de prevención y lucha contra la utilización de niños, niñas y adolescentes en la pornografía. El ICBF establecerá las características del aviso, y determinará el contenido de la leyenda. Será responsabilidad de los establecimientos anteriormente mencionados, elaborar el aviso de acuerdo a las condiciones estandarizadas que determine el ICBF. Las autoridades de Policía cerrarán hasta por un término de 7 días a todo establecimiento que cobije esta medida y que no tenga ubicado el afiche, hasta tanto cumpla con la ubicación del aviso.

CAPITULO II

Extinción de dominio y otras medidas de control en casos de explotación sexual de niños, niñas y adolescentes

Artículo 9°. *Normas sobre extinción de dominio.* La Ley 793 del 27 de diciembre de 2002 por la cual se deroga la Ley 333 de 1996 y se establecen las reglas que gobiernan la extinción de dominio, y normas que la modifiquen, se aplicará a los hoteles, pensiones, hostales, residencias, apartahoteles y a los demás establecimientos que presten el servicio de hospedaje, cuando tales inmuebles hayan sido utilizados para la comisión de actividades de utilización sexual de niños, niñas y adolescentes.

Los bienes, rendimientos y frutos que generen los inmuebles de que trata esta norma, y cuya extinción de dominio se haya decretado conforme a las leyes, deberán destinarse a la financiación del Fondo contra la Explotación Sexual de Menores. Los recaudos generados en virtud de la destinación provisional de tales bienes se destinarán en igual forma.

Artículo 10. *Procuraduría preventiva en el cumplimiento de la Ley 679 de 2001.* El Procurador General de la Nación sin perjuicio de su autonomía constitucional, ejercerá procuraduría preventiva frente a las autoridades de todo nivel territorial encargadas de la construcción, adaptación y ejecución de protocolos y lineamientos nacionales para la atención a víctimas de explotación sexual comercial de niñas, niños y adolescentes, acorde con sus características y nivel de vulneración de sus derechos.

Artículo 11. *Control de resultados de la Fiscalía.* En el ejercicio del control externo de los resultados de la gestión de la Fiscalía General de la Nación a cargo del Consejo Superior de la Judicatura se examinarán las acciones ejecutadas en la Fiscalía, en el contexto del nuevo sistema penal acusatorio, relacionadas con la representación judicial de las víctimas menores de edad dentro de los procesos penales relacionados con víctimas de delitos contra la libertad, integridad y formación sexuales, y la sanción penal de hechos punibles asociados a la utilización o explotación sexual de niños, niñas y adolescentes.

CAPITULO III

Normas sobre información

Artículo 12. *Informe a pasajeros.* Mediante reglamentos aeronáuticos o resoluciones administrativas conducentes, la Aeronáutica Civil adoptará disposiciones concretas y permanentes que aseguren que toda aerolínea nacional y extranjera informe a sus pasajeros, que en Colombia existen disposiciones legales que previenen y castigan el turismo sexual con niños, niñas y adolescentes.

El incumplimiento de este deber por parte de las Aerolíneas y empresas aéreas, dará lugar a las sanciones administrativas que se derivan del incumplimiento de reglamentos aeronáuticos.

El Ministerio de Transporte dictará las resoluciones administrativas del caso, con el mismo fin para el control y sanción por incumplimiento de este deber por parte de las empresas de transporte terrestre internacional y nacional de pasajeros.

Artículo 13. *Normas sobre información estadística.* El artículo 36 de la Ley 679 de 2001 quedará así:

Artículo 36. *Investigación estadística.* Con el fin de producir y difundir información estadística sobre la explotación sexual de niños, niñas y adolescentes, así como unificar variables, el DANE explorará y probará metodologías estadísticas técnicamente viables, procesará y consolidará información mediante un formato único que deben diligenciar las organizaciones gubernamentales y no gubernamentales, y realizar al menos cada dos años investigaciones que permitan recaudar información estadística sobre:

- Magnitud aproximada de los niños, niñas y adolescentes menores de 18 años explotados sexual y comercialmente.

- Caracterización de la población menor de 18 años en condición de explotación sexual comercial.

- Lugares o áreas de mayor incidencia.

- Formas de remuneración.

- Formas de explotación sexual.

- Factores de riesgo que propician la explotación sexual de los menores de 18 años.

- Perfiles de hombres y mujeres que compran sexo y de quienes se encargan de la intermediación.

El ICBF podrá sugerir al DANE recabar información estadística sobre algún otro dato relacionado con la problemática. Los gobernadores y alcaldes distritales y municipales, así como las autoridades indígenas, prestarán su concurso al DANE para la realización de las investigaciones.

Toda persona natural o jurídica de cualquier orden o naturaleza, domiciliada o residente en territorio nacional, está obligada a suministrar datos al DANE en el desarrollo de su investigación. Los datos acopiados no podrán darse a conocer al público ni a las entidades u organismos oficiales, ni a las autoridades públicas, sino únicamente en resúmenes numéricos y/o cualitativos, que impidan deducir de ellos información de carácter individual que pudiera utilizarse para fines de discriminación.

El DANE impondrá sanción de multa de entre uno (1) y cincuenta (50) salarios mínimos legales mensuales vigentes a toda persona natural o jurídica, o entidad pública que incumpla lo dispuesto en esta norma, o que obstaculice la realización de la investigación, previa la aplicación del procedimiento establecido en el Código Contencioso Administrativo, con observancia del debido proceso y criterios de adecuación, proporcionalidad y reincidencia.

Artículo 14. *Informe anual a cargo del ICBF.* El ICBF preparará anualmente un informe que deberá ser presentado al Congreso de la República dentro de los primeros cinco (5) días del segundo período de cada legislatura, por el director del Instituto Colombiano de Bienestar Familiar.

El informe deberá contener, cuando menos, los siguientes aspectos:

1. Análisis y diagnóstico de la situación de la infancia y la adolescencia en el país.

2. Los resultados de las políticas, objetivos, programas y planes durante el período fiscal anterior.

3. La evaluación del funcionamiento de cada una de las Direcciones Regionales en la cual se incluyen niveles de productividad e indicadores de desempeño.

4. Las políticas, objetivos y planes que desarrollará a corto, mediano y largo plazo el ICBF para dar cumplimiento al Código de la Infancia y la Adolescencia y a la Ley 679 de 2001 y sus reformas.

5. El plan de inversiones y el presupuesto de funcionamiento para el año en curso, incluido lo relacionado con el Fondo contra la Explotación Sexual de Menores, de que trata el artículo 24 de la Ley 679 de 2001.

6. La descripción del cumplimiento de metas, e identificación de las metas atrasadas, de todas las entidades que tienen competencias asignadas en el Código de la Infancia y la Adolescencia y en la Ley 679 y sus reformas.

7. El resumen de los problemas que en la coyuntura afectan los Programas de Prevención y lucha Contra la Explotación Sexual de Niños, Niñas y Adolescentes, y de las necesidades que a juicio del ICBF existan en materia de personal, instalaciones físicas y demás recursos para el correcto desempeño de las funciones de que trata la Ley 679.

Parágrafo 1°. Con el fin de explicar el contenido del informe, el Director del ICBF concurrirá a las Comisiones Primeras de Senado y Cámara de Representantes en sesiones exclusivas convocadas para tal efecto, sin perjuicio de las competencias que, en todo caso, conserva el Congreso de la República para citar e invitar en cualquier momento a los servidores públicos del Estado, para conocer sobre el Estado de la aplicación de la Ley de Infancia y Adolescencia y de la Ley 679 de 2001.

Parágrafo 2°. Copia de este informe será remitido al Procurador General de la Nación para lo de su competencia en materia preventiva y de sanción disciplinaria.

Artículo 15. *Compilación de información a cargo de la Defensoría, con cargo a recursos de la Imprenta Nacional.* La Defensoría del Pueblo producirá anualmente una compilación de las estadísticas básicas, así como de los principales diagnósticos, investigaciones y análisis que se produzcan a nivel nacional en el ámbito no gubernamental sobre explotación sexual de niños, niñas y adolescentes. La compilación será publicada por la Imprenta Nacional de Colombia, con cargo a su presupuesto. La compilación vendrá precedida de una introducción, en la cual se explicarán los criterios que se usaron para priorizar y efectuar la selección, y se señalarán determinadas cuestiones específicas que deban ser examinadas por autoridades y particulares relacionados con la ejecución de la Ley 679 de 2001.

La compilación anual será distribuida con el criterio estratégico que defina la Defensoría, y estará disponible en forma impresa y magnética. En todo caso será accesible al público en internet.

La Defensoría publicará informes defensoriales sobre la temática de la Ley 679 de 2001 y demás normas que la modifiquen.

Artículo 16. *Deber de reportar información.* A instancia del ICBF, toda institución de nivel nacional, territorial o local comprometida en desarrollo del Plan Nacional contra la Explotación Sexual Comercial Infantil de Niños, Niñas y Adolescentes, o de los

planes correspondientes en su nivel, deberá reportar los avances, limitaciones y proyecciones de aquello que le compete, con la frecuencia, en los plazos y las condiciones formales que señale el Instituto.

Artículo 17. *Sistema de información delitos sexuales.* En aplicación del artículo 257-5 de la Constitución, el Sistema de Información sobre Delitos Sexuales contra Menores de que trata el artículo 15 de la Ley 679 de 2001 estará a cargo del Consejo Superior de la Judicatura, quien convocará al Ministerio del Interior y de Justicia, al Departamento Administrativo de Seguridad, DAS, a la Policía, al Instituto Colombiano de Bienestar Familiar, a Medicina Legal y a la Fiscalía General de la Nación para el efecto. El sistema se financiará con cargo al presupuesto del Consejo Superior.

El Consejo Superior reglamentará el sistema de información de tal manera que exista una aproximación unificada a los datos mediante manuales o instructivos uniformes de provisión de información. El Consejo también fijará responsabilidades y competencias administrativas precisas en relación con la operación y alimentación del sistema, incluyendo las de las autoridades que cumplen funciones de Policía Judicial; y dispondrá sobre la divulgación de los reportes correspondientes a las entidades encargadas de la definición de políticas asociadas a la Ley 679 de 2001. Asimismo, mantendrá actualizado el sistema con base en la información que le sea suministrada.

Artículo 18. *Capítulo nuevo en el Informe Anual al Congreso del Consejo Superior de la Judicatura.* En su informe anual al Congreso, el Consejo Superior de la Judicatura incluirá un capítulo sobre las acciones ejecutadas en la Rama Judicial, en todas las jurisdicciones, relacionadas con la protección constitucional de los niños, niñas y adolescentes víctimas de delitos contra la libertad, integridad y formación sexuales, y la sanción de conductas asociadas a utilización o explotación sexual de menores.

CAPITULO IV

Criterios de clasificación de páginas y acciones de cooperación internacional

Artículo 19. *Documento de criterios de clasificación de páginas en Internet.* El documento de criterios de clasificación de páginas en Internet con contenidos de pornografía infantil y de recomendaciones al gobierno será actualizado cada dos años, a fin de revisar la vigencia doctrinal de sus definiciones, actualizar los criterios sobre tipos y efectos de la pornografía infantil, asegurar la actualidad de los marcos

tecnológicos de acción, así como la renovación de las recomendaciones para la prevención y la idoneidad y eficiencia de las medidas técnicas y administrativas destinadas a prevenir el acceso de niños, niñas y adolescentes a cualquier modalidad de información pornográfica contenida en Internet o cualquier otra red global de información.

La comisión de expertos será convocada cada dos (2) años en las mismas condiciones y con las mismas competencias fijadas en los artículos 4° y 5° de la Ley 679 de 2001 y sus reformas.

El documento de la comisión será criterio auxiliar en las investigaciones administrativas y judiciales, y servirá de base para políticas públicas preventivas.

Artículo 20. *Eventos de cooperación internacional.* En un plazo no mayor a cinco años, el Ministerio de Relaciones Exteriores, en coordinación con el ICBF, realizará el primer evento de cooperación internacional de que trata el artículo 13 de la Ley 679, en la forma de una cumbre regional que incluya a los países de América Latina y el Caribe, a fin de diagnosticar y analizar la problemática del turismo sexual con niños, niñas y adolescentes en la región, y proponer recomendaciones concretas de orden nacional, regional, o mundial para la lucha contra el flagelo. La realización de estos eventos será sucesiva.

CAPITULO V

Normas de financiación

Artículo 21. *Fondo contra la Explotación Sexual*. Subróguese el parágrafo 3° del artículo 24 de la Ley 679 de 2001, y en su lugar se dispone:

Parágrafo 3°. Corresponde al ICBF elaborar anualmente el proyecto de presupuesto del Fondo de que trata el presente artículo, que deberá remitirse al Gobierno Nacional, quien deberá incorporarlo en el proyecto de ley anual de presupuesto. Esta responsabilidad se asumirá conjuntamente con el Ministerio de la Protección Social y el apoyo de la Comisión Interinstitucional integrada por las agencias oficiales responsables de la aplicación de la Ley 679.

Cada año, simultáneamente con la adjudicación de la ponencia del Proyecto de Ley Anual de Presupuesto, la Mesa Directiva de la comisión o comisiones constitucionales respectivas, oficiarán al ICBF para que se pronuncie por escrito sobre lo inicialmente propuesto al Gobierno y lo finalmente incorporado al proyecto de ley anual. El informe será entregado de manera formal a los ponentes para su estudio y consideración.

Los Secretarios de las Comisiones Constitucionales respectivas tendrán la responsabilidad de hacer las advertencias sobre el particular.

Artículo 22. *Competencia en materia de impuestos.* La competencia para la reglamentación y recaudo del impuesto a videos para adultos de que trata el artículo 22 de la Ley 679 de 2001 estará a cargo de la Dirección de Impuestos y Aduanas Nacionales.

El recaudo del impuesto consagrado en el artículo 23 de la Ley 679 de 2001 será responsabilidad de la Dirección de Impuestos y Aduanas Nacionales en concurso con la Aeronáutica Civil.

La reglamentación de estos impuestos se hará dentro de los seis meses siguientes a la vigencia de esta ley, sin que por ello el Gobierno afecte su potestad reglamentaria.

CAPITULO VI

Tipos penales de turismo sexual y almacenamiento e intercambio de pornografía infantil

Artículo 23. *Turismo sexual.* El artículo 219 de la Ley 599 de 2000 recupera su vigencia, y quedará así:

Turismo sexual. El que dirija, organice o promueva actividades turísticas que incluyan la utilización sexual de menores de edad incurrirá en prisión de cuatro (4) a ocho (8) años.

La pena se aumentará en la mitad cuando la conducta se realizare con menor de doce (12) años.

Artículo 24. El artículo 218 de la ley 599 quedará así:

Artículo 218. *Pornografía con personas menores de 18 años.* El que fotografíe, filme, grabe, produzca, divulgue, ofrezca, venda, compre, posea, porte, almacene, trasmita o exhiba, por cualquier medio, para uso personal o intercambio, representaciones reales de actividad sexual que involucre persona menor de 18 años de edad, incurrirá en prisión de 10 a 20 años y multa de 150 a 1.500 salarios mínimos legales mensuales vigentes.

Igual pena se aplicará a quien alimente con pornografía infantil bases de datos de Internet, con o sin fines de lucro.

La pena se aumentará de una tercera parte a la mitad cuando el responsable sea integrante de la familia de la víctima.

Artículo 25. *Vigilancia y Control.* La Policía Nacional tendrá además de las funciones constitucionales y legales las siguientes:

Los comandantes de estación y subestación de acuerdo con su competencia, podrán ordenar el cierre temporal de los establecimientos abiertos al público de acuerdo con los procedimientos señalados en el Código Nacional de Policía, cuando

el propietario o responsable de su explotación económica realice alguna de las siguientes conductas:

1. Alquile, distribuya, comercialice, exhiba, o publique textos, imágenes, documentos, o archivos audiovisuales de contenido pornográfico a menores de 14 años a través de internet, salas de video, juegos electrónicos o similares.

2. En caso de hoteles, pensiones, hostales, residencias, apartahoteles y demás establecimientos que presten servicios de hospedaje, de acuerdo con los procedimientos señalados en el Código Nacional de Policía, se utilicen o hayan sido utilizados para la comisión de actividades sexuales de/o con niños, niñas y adolescentes, sin perjuicios de las demás sanciones que ordena la ley.

3. Las empresas comercializadoras de computadores que no entreguen en lenguaje accesible a los compradores instrucciones o normas básicas de seguridad en línea para niños, niñas y adolescentes.

Artículo 26. En aplicación del numeral 4 del artículo 95 de la Constitución, y dentro de los espacios reservados por ley a mensajes institucionales, la CNTV reservará el tiempo semanal que defina su Junta Directiva, para la divulgación de casos de menores desaparecidos o secuestrados. La CNTV coordinará con el ICBF y la Fiscalía General de la Nación para este propósito.

Artículo 27. *Del Comité Nacional Interinstitucional.* Para ejecutar la política pública de prevención y erradicación de la ESCNNA se crea el Comité Nacional Interinstitucional como ente integrante y consultor del Consejo Nacional de Política Social.

El Comité estará integrado por los siguientes miembros:

a) Entidades estatales:

Ministerio de la Protección Social, quién lo presidirá.

Ministerio del Interior y de Justicia.

Ministerio de Educación.

Ministerio de Comunicaciones.

Ministerio de Comercio, Industria y Turismo.

Ministerio de Relaciones Exteriores.

Instituto Colombiano de Bienestar Familiar.

Departamento Administrativo de Seguridad.

Policía Nacional (Policía de Infancia y Adolescencia, Policía de Turismo, Dijín).

Fiscalía General de la Nación.

Departamento Nacional de Estadística.

Programa Presidencial para el Sistema Nacional de Juventud "Colombia Joven".

b) Invitados permanentes

1. Procuraduría General de la Nación.

2. Defensoría del Pueblo.

3. ONG que trabajan el tema.

4. Representantes de la empresa privada.

5. Representante de las organizaciones de niños, niñas y adolescentes.

6. Representantes de los organismos de cooperación internacional que impulsan y apoyan el Plan.

Artículo 28. *Vigencia y derogatorias.* La presente ley rige a partir de la fecha de su publicación y deroga las normas que le sean contrarias.

El Presidente del honorable Senado de la República,

Hernán Francisco Andrade Serrano.

El Secretario General del honorable Senado de la República,

Emilio Ramón Otero Dajud.

El Presidente de la honorable Cámara de Representantes,

Germán Varón Cotrino.

El Secretario General de la honorable Cámara de Representantes,

Jesús Alfonso Rodríguez Camargo.

REPUBLICA DE COLOMBIA - GOBIERNO NACIONAL

Publíquese y cúmplase.

Dada en Bogotá, D. C., a 21 de julio de 2009.

ÁLVARO URIBE VÉLEZ

El Ministro del Interior y de Justicia,

Fabio Valencia Cossio.

El Ministro de Hacienda y Crédito Público,

Oscar Iván Zuluaga Escobar.

El Ministro de la Protección Social,

Diego Palacio Betancourt.

El Ministro del Comercio, Industria y Turismo,

Luis Guillermo Plata Páez.

La Ministra de Comunicaciones,

María del Rosario Guerra de la Espriella.

NOTA: Publicada en el Diario Oficial 47.417 de julio 21 de 2009.

2.2.7 Ley Estatutaria 1266 DE 2008

(Diciembre 31)

Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

El Congreso de la República

DECRETA:

Ver el art. 15, Constitución Política de 1991

Artículo 1°. *Objeto*. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países.

Artículo 2°. *Ámbito de aplicación*. La presente ley se aplica a todos los datos de información personal registrados en un banco de datos, sean estos administrados por entidades de naturaleza pública o privada.

Esta ley se aplicará sin perjuicio de normas especiales que disponen la confidencialidad o reserva de ciertos datos o información registrada en bancos de datos de naturaleza pública, para fines estadísticos, de investigación o sanción de delitos o para garantizar el orden público.

Se exceptúan de esta ley las bases de datos que tienen por finalidad producir la Inteligencia de Estado por parte del Departamento Administrativo de Seguridad, DAS, y de la Fuerza Pública para garantizar la seguridad nacional interna y externa.

Los registros públicos a cargo de las cámaras de comercio se regirán exclusivamente por las normas y principios consagrados en las normas especiales que las regulan.

Igualmente, quedan excluidos de la aplicación de la presente ley aquellos datos mantenidos en un ámbito exclusivamente personal o doméstico y aquellos que

circulan internamente, esto es, que no se suministran a otras personas jurídicas o naturales.

Artículo 3°. *Definiciones*. Para los efectos de la presente ley, se entiende por:

a) Titular de la información. Es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías a que se refiere la presente ley;

b) Fuente de información. Es la persona, entidad u organización que recibe o conoce datos personales de los titulares de la información, en virtud de una relación comercial o de servicio o de cualquier otra índole y que, en razón de autorización legal o del titular, suministra esos datos a un operador de información, el que a su vez los entregará al usuario final. Si la fuente entrega la información directamente a los usuarios y no, a través de un operador, aquella tendrá la doble condición de fuente y operador y asumirá los deberes y responsabilidades de ambos. La fuente de la información responde por la calidad de los datos suministrados al operador la cual, en cuanto tiene acceso y suministra información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstas para garantizar la protección de los derechos del titular de los datos;

c) Operador de información. Se denomina operador de información a la persona, entidad u organización que recibe de la fuente datos personales sobre varios titulares de la información, los administra y los pone en conocimiento de los usuarios bajo los parámetros de la presente ley. Por tanto, el operador, en cuanto tiene acceso a información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos. Salvo que el operador sea la misma fuente de la información, este no tiene relación comercial o de servicio con el titular y por ende no es responsable por la calidad de los datos que le sean suministrados por la fuente;

d) Usuario. El usuario es la persona natural o jurídica que, en los términos y circunstancias previstos en la presente ley, puede acceder a información personal de uno o varios titulares de la información suministrada por el operador o por la fuente, o directamente por el titular de la información. El usuario, en cuanto tiene acceso a información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos. En el caso en que el usuario a su vez entregue la información directamente a un operador, aquella tendrá la doble condición de usuario y fuente, y asumirá los deberes y responsabilidades de ambos;

e) Dato personal. Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la presente ley. Cuando en la presente ley se haga referencia a un dato, se presume que se trata de uso personal. Los datos personales pueden ser públicos, semiprivados o privados;

f) Dato público. Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas;

g) Dato semiprivado. Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV de la presente ley.

h) Dato privado. Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

i) Agencia de Información Comercial. Es toda empresa legalmente constituida que tenga como actividad principal la recolección, validación y procesamiento de información comercial sobre las empresas y comerciantes específicamente solicitadas por sus clientes, entendiéndose por información comercial aquella información histórica y actual relativa a la situación financiera, patrimonial, de mercado, administrativa, operativa, sobre el cumplimiento de obligaciones y demás información relevante para analizar la situación integral de una empresa. Para los efectos de la presente ley, las agencias de información comercial son operadores de información y fuentes de información.

Parágrafo: A las agencias de información comercial, así como a sus fuentes o usuarios, según sea el caso, no se aplicarán las siguientes disposiciones de la presente ley: numerales 2 y 6 del artículo 8°, artículo 12, y artículo 14.

j) Información financiera, crediticia, comercial, de servicios y la proveniente de terceros países.

Para todos los efectos de la presente ley se entenderá por información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, aquella referida al nacimiento, ejecución y extinción de obligaciones dinerarias, independientemente de la naturaleza del contrato que les dé origen.

Artículo 4°. *Principios de la administración de datos*. En el desarrollo, interpretación y aplicación de la presente ley, se tendrán en cuenta, de manera armónica e integral, los principios que a continuación se establecen:

a) Principio de veracidad o calidad de los registros o datos. La información contenida en los bancos de datos debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el registro y divulgación de datos parciales, incompletos, fraccionados o que induzcan a error;

b) Principio de finalidad. La administración de datos personales debe obedecer a una finalidad legítima de acuerdo con la Constitución y la ley. La finalidad debe informársele al titular de la información previa o concomitantemente con el

otorgamiento de la autorización, cuando ella sea necesaria o en general siempre que el titular solicite información al respecto;

c) Principio de circulación restringida. La administración de datos personales se sujeta a los límites que se derivan de la naturaleza de los datos, de las disposiciones de la presente ley y de los principios de la administración de datos personales especialmente de los principios de temporalidad de la información y la finalidad del banco de datos.

Los datos personales, salvo la información pública, no podrán ser accesibles por Internet o por otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o los usuarios autorizados conforme a la presente ley;

d) Principio de temporalidad de la información. La información del titular no podrá ser suministrada a usuarios o terceros cuando deje de servir para la finalidad del banco de datos;

e) Principio de interpretación integral de derechos constitucionales. La presente ley se interpretará en el sentido de que se amparen adecuadamente los derechos constitucionales, como son el hábeas data, el derecho al buen nombre, el derecho a la honra, el derecho a la intimidad y el derecho a la información. Los derechos de los titulares se interpretarán en armonía y en un plano de equilibrio con el derecho a la información previsto en el artículo 20 de la Constitución y con los demás derechos constitucionales aplicables;

f) Principio de seguridad. La información que conforma los registros individuales constitutivos de los bancos de datos a que se refiere la ley, así como la resultante de las consultas que de ella hagan sus usuarios, se deberá manejar con las medidas técnicas que sean necesarias para garantizar la seguridad de los registros evitando su adulteración, pérdida, consulta o uso no autorizado;

g) Principio de confidencialidad. Todas las personas naturales o jurídicas que intervengan en la administración de datos personales que no tengan la naturaleza de públicos están obligadas en todo tiempo a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende la administración de datos, pudiendo sólo realizar suministro o comunicación de datos cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma.

Artículo 5°. *Circulación de información*. La información personal recolectada o suministrada de conformidad con lo dispuesto en la ley a los operadores que haga parte del banco de datos que administra, podrá ser entregada de manera verbal, escrita, o puesta a disposición de las siguientes personas y en los siguientes términos:

a) A los titulares, a las personas debidamente autorizadas por estos y a sus causahabientes mediante el procedimiento de consulta previsto en la presente ley.

b) A los usuarios de la información, dentro de los parámetros de la presente ley.

c) A cualquier autoridad judicial, previa orden judicial.

d) A las entidades públicas del poder ejecutivo, cuando el conocimiento de dicha información corresponda directamente al cumplimiento de alguna de sus funciones.

e) A los órganos de control y demás dependencias de investigación disciplinaria, fiscal, o administrativa, cuando la información sea necesaria para el desarrollo de una investigación en curso.

f) A otros operadores de datos, cuando se cuente con autorización del titular, o cuando sin ser necesaria la autorización del titular el banco de datos de destino tenga la misma finalidad o una finalidad que comprenda la que tiene el operador que entrega los datos. Si el receptor de la información fuere un banco de datos extranjero, la entrega sin autorización del titular sólo podrá realizarse dejando constancia escrita de la entrega de la información y previa verificación por parte del operador de que las leyes del país respectivo o el receptor otorgan garantías suficientes para la protección de los derechos del titular.

g) A otras personas autorizadas por la ley.

TITULO II

DERECHOS DE LOS TITULARES DE LA INFORMACION

Artículo 6°. *Derechos de los titulares de la información.* Los titulares tendrán los siguientes derechos:

1. Frente a los operadores de los bancos de datos:

1.1 Ejercer el derecho fundamental al hábeas data en los términos de la presente ley, mediante la utilización de los procedimientos de consultas o reclamos, sin perjuicio de los demás mecanismos constitucionales y legales.

1.2 Solicitar el respeto y la protección de los demás derechos constitucionales o legales, así como de las demás disposiciones de la presente ley, mediante la utilización del procedimiento de reclamos y peticiones.

1.3 Solicitar prueba de la certificación de la existencia de la autorización expedida por la fuente o por el usuario.

1.4 Solicitar información acerca de los usuarios autorizados para obtener información.

Parágrafo. La administración de información pública no requiere autorización del titular de los datos, pero se sujeta al cumplimiento de los principios de la administración de datos personales y a las demás disposiciones de la presente ley.

La administración de datos semiprivados y privados requiere el consentimiento previo y expreso del titular de los datos, salvo en el caso del dato financiero, crediticio, comercial, de servicios y el proveniente de terceros países el cual no requiere autorización del titular. En todo caso, la administración de datos

semiprivados y privados se sujeta al cumplimiento de los principios de la administración de datos personales y a las demás disposiciones de la presente ley.

2. Frente a las fuentes de la información:

2.1 Ejercer los derechos fundamentales al hábeas data y de petición, cuyo cumplimiento se podrá realizar a través de los operadores, conforme lo previsto en los procedimientos de consultas y reclamos de esta ley, sin perjuicio de los demás mecanismos constitucionales o legales.

2.2 Solicitar información o pedir la actualización o rectificación de los datos contenidos en la base de datos, lo cual realizará el operador, con base en la información aportada por la fuente, conforme se establece en el procedimiento para consultas, reclamos y peticiones.

2.3 Solicitar prueba de la autorización, cuando dicha autorización sea requerida conforme lo previsto en la presente ley.

3. Frente a los usuarios:

3.1 Solicitar información sobre la utilización que el usuario le está dando a la información, cuando dicha información no hubiere sido suministrada por el operador.

3.2 Solicitar prueba de la autorización, cuando ella sea requerida conforme lo previsto en la presente ley.

Parágrafo. Los titulares de información financiera y crediticia tendrán adicionalmente los siguientes derechos:

Podrán acudir ante la autoridad de vigilancia para presentar quejas contra las fuentes, operadores o usuarios por violación de las normas sobre administración de la información financiera y crediticia.

Así mismo, pueden acudir ante la autoridad de vigilancia para pretender que se ordene a un operador o fuente la corrección o actualización de sus datos personales, cuando ello sea procedente conforme lo establecido en la presente ley.

TITULO III

DEBERES DE LOS OPERADORES, LAS FUENTES Y LOS USUARIOS DE INFORMACION

Artículo 7°. *Deberes de los operadores de los bancos de datos*. Sin perjuicio del cumplimiento de las demás disposiciones contenidas en la presente ley y otras que rijan su actividad, los operadores de los bancos de datos están obligados a:

1. Garantizar, en todo tiempo al titular de la información, el pleno y efectivo ejercicio del derecho de hábeas data y de petición, es decir, la posibilidad de conocer la información que sobre él exista o repose en el banco de datos, y solicitar la

actualización o corrección de datos, todo lo cual se realizará por conducto de los mecanismos de consultas o reclamos, conforme lo previsto en la presente ley.

2. Garantizar, que, en la recolección, tratamiento y circulación de datos, se respetarán los demás derechos consagrados en la ley.

3. Permitir el acceso a la información únicamente a las personas que, de conformidad con lo previsto en esta ley, pueden tener acceso a ella.

4. Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos por parte de los titulares.

5. Solicitar la certificación a la fuente de la existencia de la autorización otorgada por el titular, cuando dicha autorización sea necesaria, conforme lo previsto en la presente ley.

6. Conservar con las debidas seguridades los registros almacenados para impedir su deterioro, pérdida, alteración, uso no autorizado o fraudulento.

7. Realizar periódica y oportunamente la actualización y rectificación de los datos, cada vez que le reporten novedades las fuentes, en los términos de la presente ley.

8. Tramitar las peticiones, consultas y los reclamos formulados por los titulares de la información, en los términos señalados en la presente ley.

9. Indicar en el respectivo registro individual que determinada información se encuentra en discusión por parte de su titular, cuando se haya presentado la solicitud de rectificación o actualización de la misma y no haya finalizado dicho trámite, en la forma en que se regula en la presente ley.

10. Circular la información a los usuarios dentro de los parámetros de la presente ley.

11. Cumplir las instrucciones y requerimientos que la autoridad de vigilancia imparta en relación con el cumplimiento de la presente ley.

12. Los demás que se deriven de la Constitución o de la presente ley.

Artículo 8°. *Deberes de las fuentes de la información*. Las fuentes de la información deberán cumplir las siguientes obligaciones, sin perjuicio del cumplimiento de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

1. Garantizar que la información que se suministre a los operadores de los bancos de datos o a los usuarios sea veraz, completa, exacta, actualizada y comprobable.

2. Reportar, de forma periódica y oportuna al operador, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada.

3. Rectificar la información cuando sea incorrecta e informar lo pertinente a los operadores.

4. Diseñar e implementar mecanismos eficaces para reportar oportunamente la información al operador.

5. Solicitar, cuando sea del caso, y conservar copia o evidencia de la respectiva autorización otorgada por los titulares de la información, y asegurarse de no suministrar a los operadores ningún dato cuyo suministro no esté previamente autorizado, cuando dicha autorización sea necesaria, de conformidad con lo previsto en la presente ley.

6. Certificar, semestralmente al operador, que la información suministrada cuenta con la autorización de conformidad con lo previsto en la presente ley.

7. Resolver los reclamos y peticiones del titular en la forma en que se regula en la presente ley.

8. Informar al operador que determinada información se encuentra en discusión por parte de su titular, cuando se haya presentado la solicitud de rectificación o actualización de la misma, con el fin de que el operador incluya en el banco de datos una mención en ese sentido hasta que se haya finalizado dicho trámite.

9. Cumplir con las instrucciones que imparta la autoridad de control en relación con el cumplimiento de la presente ley.

10. Los demás que se deriven de la Constitución o de la presente ley.

Artículo 9°. *Deberes de los usuarios*. Sin perjuicio del cumplimiento de las disposiciones contenidas en la presente ley y demás que rijan su actividad, los usuarios de la información deberán:

1. Guardar reserva sobre la información que les sea suministrada por los operadores de los bancos de datos, por las fuentes o los titulares de la información y utilizar la información únicamente para los fines para los que le fue entregada, en los términos de la presente ley.

2. Informar a los titulares, a su solicitud, sobre la utilización que le está dando a la información.

3. Conservar con las debidas seguridades la información recibida para impedir su deterioro, pérdida, alteración, uso no autorizado o fraudulento.

4. Cumplir con las instrucciones que imparta la autoridad de control, en relación con el cumplimiento de la presente ley.

5. Los demás que se deriven de la Constitución o de la presente ley.

TITULO IV

DE LOS BANCOS DE DATOS DE INFORMACION FINANCIERA, CREDITICIA, COMERCIAL, DE SERVICIOS Y LA PROVENIENTE DE TERCEROS PAISES

Artículo 10. *Principio de favorecimiento a una actividad de interés público*. La actividad de administración de información financiera, crediticia, comercial, de

servicios y la proveniente de terceros países está directamente relacionada y favorece una actividad de interés público, como lo es la actividad financiera propiamente, por cuanto ayuda a la democratización del crédito, promueve el desarrollo de la actividad de crédito, la protección de la confianza pública en el sistema financiero y la estabilidad del mismo, y genera otros beneficios para la economía nacional y en especial para la actividad financiera, crediticia, comercial y de servicios del país.

Parágrafo 1°. La administración de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, por parte de fuentes, usuarios y operadores deberá realizarse de forma que permita favorecer los fines de expansión y democratización del crédito. Los usuarios de este tipo de información deberán valorar este tipo de información en forma concurrente con otros factores o elementos de juicio que técnicamente inciden en el estudio de riesgo y el análisis crediticio, y no podrán basarse exclusivamente en la información relativa al incumplimiento de obligaciones suministrada por los operadores para adoptar decisiones frente a solicitudes de crédito.

La Superintendencia Financiera de Colombia podrá imponer las sanciones previstas en la presente ley a los usuarios de la información que nieguen una solicitud de crédito basados exclusivamente en el reporte de información negativa del solicitante.

Parágrafo 2°. La consulta de la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países por parte del titular, será gratuita al menos una (1) vez cada mes calendario.

Artículo 11. *Requisitos especiales para los operadores*. Los operadores de bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países que funcionen como entes independientes a las fuentes de la información, deberán cumplir con los siguientes requisitos especiales de funcionamiento:

1. Deberán constituirse como sociedades comerciales, entidades sin ánimo de lucro, o entidades cooperativas.

2. Deberán contar con un área de servicio al titular de la información, para la atención de peticiones, consultas y reclamos.

3. Deberán contar con un sistema de seguridad y con las demás condiciones técnicas suficientes para garantizar la seguridad y actualización de los registros, evitando su adulteración, pérdida, consulta o uso no autorizado conforme lo previsto en la presente ley.

4. Deberán actualizar la información reportada por las fuentes con una periodicidad no superior a diez (10) días calendario contados a partir del recibo de la misma.

Artículo 12. *Requisitos especiales para fuentes*. Reglamentado por el Decreto Nacional 2952 de 2010. Las fuentes deberán actualizar mensualmente la

información suministrada al operador, sin perjuicio de lo dispuesto en el Título III de la presente ley.

El reporte de información negativa sobre incumplimiento de obligaciones de cualquier naturaleza, que hagan las fuentes de información a los operadores de bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, sólo procederá previa comunicación al titular de la información, con el fin de que este pueda demostrar o efectuar el pago de la obligación, así como controvertir aspectos tales como el monto de la obligación o cuota y la fecha de exigibilidad. Dicha comunicación podrá incluirse en los extractos periódicos que las fuentes de información envíen a sus clientes.

En todo caso, las fuentes de información podrán efectuar el reporte de la información transcurridos veinte (20) días calendario siguientes a la fecha de envío de la comunicación en la última dirección de domicilio del afectado que se encuentre registrada en los archivos de la fuente de la información y sin perjuicio, si es del caso, de dar cumplimiento a la obligación de informar al operador, que la información se encuentra en discusión por parte de su titular, cuando se haya presentado solicitud de rectificación o actualización y está aún no haya sido resuelta.

Artículo 13. *Permanencia de la información*. Reglamentado por el Decreto Nacional 2952 de 2010. La información de carácter positivo permanecerá de manera indefinida en los bancos de datos de los operadores de información.

Los datos cuyo contenido haga referencia al tiempo de mora, tipo de cobro, estado de la cartera, y en general, aquellos datos referentes a una situación de incumplimiento de obligaciones, se regirán por un término máximo de permanencia, vencido el cual deberá ser retirada de los bancos de datos por el operador, de forma que los usuarios no puedan acceder o consultar dicha información. El término de permanencia de esta información será de cuatro (4) años contados a partir de la fecha en que sean pagadas las cuotas vencidas o sea pagada la obligación vencida.

Artículo 14. *Contenido de la información*. El Gobierno Nacional establecerá la forma en la cual los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deberán presentar la información de los titulares de la información. Para tal efecto, deberá señalar un formato que permita identificar, entre otros aspectos, el nombre completo del deudor, la condición en que actúa, esto es, como deudor principal, deudor solidario, avalista o fiador, el monto de la obligación o cuota vencida, el tiempo de mora y la fecha del pago, si es del caso.

El Gobierno Nacional al ejercer la facultad prevista en el inciso anterior deberá tener en cuenta que en el formato de reporte deberá establecer que:

a) Se presenta reporte negativo cuando la(s) persona(s) naturales o jurídicas efectivamente se encuentran en mora en sus cuotas u obligaciones.

b) Se presenta reporte positivo cuando la(s) persona(s) naturales y jurídicas están al día en sus obligaciones.

El incumplimiento de la obligación aquí prevista dará lugar a la imposición de las máximas sanciones previstas en la presente ley.

Parágrafo 1°. Para los efectos de la presente ley se entiende que una obligación ha sido voluntariamente pagada, cuando su pago se ha producido sin que medie sentencia judicial que así lo ordene.

Parágrafo 2°. Las consecuencias previstas en el presente artículo para el pago voluntario de las obligaciones vencidas, será predicable para cualquier otro modo de extinción de las obligaciones, que no sea resultado de una sentencia judicial.

Parágrafo 3°. Cuando un usuario consulte el estado de un titular en las bases de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, estas tendrán que dar información exacta sobre su estado actual, es decir, dar un reporte positivo de los usuarios que en el momento de la consulta están al día en sus obligaciones y uno negativo de los que al momento de la consulta se encuentren en mora en una cuota u obligaciones.

El resto de la información contenida en las bases de datos financieros, crediticios, comercial, de servicios y la proveniente de terceros países harán parte del historial crediticio de cada usuario, el cual podrá ser consultado por el usuario, siempre y cuando hubiere sido informado sobre el estado actual.

Parágrafo 4°. Se prohíbe la administración de datos personales con información exclusivamente desfavorable.

Artículo 15. *Acceso a la información por parte de los usuarios*. La información contenida en bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países podrá ser accedida por los usuarios únicamente con las siguientes finalidades: Como elemento de análisis para establecer y mantener una relación contractual, cualquiera que sea su naturaleza, así como para la evaluación de los riesgos derivados de una relación contractual vigente.

Como elemento de análisis para hacer estudios de mercado o investigaciones comerciales o estadísticas.

Para el adelantamiento de cualquier trámite ante una autoridad pública o una persona privada, respecto del cual dicha información resulte pertinente.

Para cualquier otra finalidad, diferente de las anteriores, respecto de la cual y en forma general o para cada caso particular se haya obtenido autorización por parte del titular de la información.

TITULO V

PETICIONES DE CONSULTAS Y RECLAMOS

Artículo 16. *Peticiones, Consultas y Reclamos*.

I. Trámite de consultas. Los titulares de la información o sus causahabientes podrán consultar la información personal del titular, que repose en cualquier banco de datos, sea este del sector público o privado. El operador deberá suministrar a estos, debidamente identificados, toda la información contenida en el registro individual o que esté vinculada con la identificación del titular.

La petición, consulta de información se formulará verbalmente, por escrito, o por cualquier canal de comunicación, siempre y cuando se mantenga evidencia de la consulta por medios técnicos.

La petición o consulta será atendida en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la petición o consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su petición, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

Parágrafo. La petición o consulta se deberá atender de fondo, suministrando integralmente toda la información solicitada.

II. Trámite de reclamos. Los titulares de la información o sus causahabientes que consideren que la información contenida en su registro individual en un banco de datos debe ser objeto de corrección o actualización podrán presentar un reclamo ante el operador, el cual será tramitado bajo las siguientes reglas:

1. La petición o reclamo se formulará mediante escrito dirigido al operador del banco de datos, con la identificación del titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y si fuere el caso, acompañando los documentos de soporte que se quieran hacer valer. En caso de que el escrito resulte incompleto, se deberá oficiar al interesado para que subsane las fallas. Transcurrido un mes desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido de la reclamación o petición.

2. Una vez recibido la petición o reclamo completo el operador incluirá en el registro individual en un término no mayor a dos (2) días hábiles una leyenda que diga "reclamo en trámite" y la naturaleza del mismo. Dicha información deberá mantenerse hasta que el reclamo sea decidido y deberá incluirse en la información que se suministra a los usuarios.

3. El término máximo para atender la petición o reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender la petición dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su

petición, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

4. En los casos en que exista una fuente de información independiente del operador, este último deberá dar traslado del reclamo a la fuente en un término máximo de dos (2) días hábiles, la cual deberá resolver e informar la respuesta al operador en un plazo máximo de diez (10) días hábiles. En todo caso, la respuesta deberá darse al titular por el operador en el término máximo de quince (15) días hábiles contados a partir del día siguiente a la fecha de presentación de la reclamación, prorrogables por ocho (8) días hábiles más, según lo indicado en el numeral anterior. Si el reclamo es presentado ante la fuente, esta procederá a resolver directamente el reclamo, pero deberá informar al operador sobre la recepción del reclamo dentro de los dos (2) días hábiles siguientes a su recibo, de forma que se pueda dar cumplimiento a la obligación de incluir la leyenda que diga "reclamo en trámite" y la naturaleza del mismo dentro del registro individual, lo cual deberá hacer el operador dentro de los dos (2) días hábiles siguientes a haber recibido la información de la fuente.

5. Para dar respuesta a la petición o reclamo, el operador o la fuente, según sea el caso, deberá realizar una verificación completa de las observaciones o planteamientos del titular, asegurándose de revisar toda la información pertinente para poder dar una respuesta completa al titular.

6. Sin perjuicio del ejercicio de la acción de tutela para amparar el derecho fundamental del hábeas data, en caso que el titular no se encuentre satisfecho con la respuesta a la petición, podrá recurrir al proceso judicial correspondiente dentro de los términos legales pertinentes para debatir lo relacionado con la obligación reportada como incumplida. La demanda deberá ser interpuesta contra la fuente de la información la cual, una vez notificada de la misma, procederá a informar al operador dentro de los dos (2) días hábiles siguientes, de forma que se pueda dar cumplimiento a la obligación de incluir la leyenda que diga "información en discusión judicial" y la naturaleza de la misma dentro del registro individual, lo cual deberá hacer el operador dentro de los dos (2) días hábiles siguientes a haber recibido la información de la fuente y por todo el tiempo que tome obtener un fallo en firme. Igual procedimiento deberá seguirse en caso que la fuente inicie un proceso judicial contra el titular de la información, referente a la obligación reportada como incumplida, y este proponga excepciones de mérito.

TITULO VI

VIGILANCIA DE LOS DESTINATARIOS DE LA LEY

Artículo 17. *Función de vigilancia*. La Superintendencia de Industria y Comercio ejercerá la función de vigilancia de los operadores, las fuentes y los usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, en cuanto se refiere a la actividad de administración de datos personales que se regula en la presente ley.

En los casos en que la fuente, usuario u operador de información sea una entidad vigilada por la Superintendencia Financiera de Colombia, esta ejercerá la vigilancia e impondrá las sanciones correspondientes, de conformidad con las facultades que le son propias, según lo establecido en el Estatuto Orgánico del Sistema Financiero y las demás normas pertinentes y las establecidas en la presente ley.

Para el ejercicio de la función de vigilancia a que se refiere el presente artículo, la Superintendencia de Industria y Comercio y la Superintendencia Financiera de Colombia, según el caso, tendrán en adición a las propias las siguientes facultades:

1. Impartir instrucciones y órdenes sobre la manera cómo deben cumplirse las disposiciones de la presente ley relacionadas con la administración de la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países fijar los criterios que faciliten su cumplimiento y señalar procedimientos para su cabal aplicación.

2. Velar por el cumplimiento de las disposiciones de la presente ley, de las normas que la reglamenten y de las instrucciones impartidas por la respectiva Superintendencia.

3. Velar porque los operadores y fuentes cuenten con un sistema de seguridad y con las demás condiciones técnicas suficientes para garantizar la seguridad y actualización de los registros, evitando su adulteración, pérdida, consulta o uso no autorizado conforme lo previsto en la presente ley.

4. Ordenar a cargo del operador, la fuente o usuario la realización de auditorías externas de sistemas para verificar el cumplimiento de las disposiciones de la presente ley.

5. Ordenar de oficio o a petición de parte la corrección, actualización o retiro de datos personales cuando ello sea procedente, conforme con lo establecido en la presente ley. Cuando sea a petición de parte, se deberá acreditar ante la Superintendencia que se surtió el trámite de un reclamo por los mismos hechos ante el operador o la fuente, y que el mismo no fue atendido o fue atendido desfavorablemente.

6. Iniciar de oficio o a petición de parte investigaciones administrativas contra los operadores, fuentes y usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, con el fin de establecer si existe responsabilidad administrativa derivada del incumplimiento de las disposiciones de la presente ley o de las órdenes o instrucciones impartidas por el organismo de vigilancia respectivo, y si es del caso imponer sanciones u ordenar las medidas que resulten pertinentes.

Artículo 18. *Sanciones*. La Superintendencia de Industria y Comercio y la Superintendencia Financiera podrán imponer a los operadores, fuentes o usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países previas explicaciones de acuerdo con el procedimiento aplicable, las siguientes sanciones:

Multas de carácter personal e institucional hasta por el equivalente a mil quinientos (1.500) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción, por violación a la presente ley, normas que la reglamenten, así como por la inobservancia de las órdenes e instrucciones impartidas por dicha Superintendencia. Las multas aquí previstas podrán ser sucesivas mientras subsista el incumplimiento que las originó.

Suspensión de las actividades del banco de datos, hasta por un término de seis (6) meses, cuando se estuviere llevando a cabo la administración de la información en violación grave de las condiciones y requisitos previstos en la presente ley, así como por la inobservancia de las órdenes e instrucciones impartidas por las Superintendencias mencionadas para corregir tales violaciones.

Cierre o clausura de operaciones del banco de datos cuando, una vez transcurrido el término de suspensión, no hubiere adecuado su operación técnica y logística, y sus normas y procedimientos a los requisitos de ley, de conformidad con lo dispuesto en la resolución que ordenó la suspensión. Cierre inmediato y definitivo de la operación de bancos de datos que administren datos prohibidos.

Artículo 19. *Criterios para graduar las sanciones*. Las sanciones por infracciones a que se refiere el artículo anterior se graduarán atendiendo los siguientes criterios, en cuanto resulten aplicables:

a) La dimensión del daño o peligro a los intereses jurídicos tutelados por la presente ley.

b) El beneficio económico que se hubiere obtenido para el infractor o para terceros, por la comisión de la infracción, o el daño que tal infracción hubiere podido causar.

c) La reincidencia en la comisión de la infracción.

d) La resistencia, negativa u obstrucción a la acción investigadora o de vigilancia de la Superintendencia de Industria y Comercio.

e) La renuencia o desacato a cumplir, con las órdenes impartidas por la Superintendencia de Industria y Comercio.

f) El reconocimiento o aceptación expresos que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar.

Artículo 20. *Régimen de transición para las Entidades de Control*. La Superintendencia de Industria y Comercio y la Superintendencia Financiera asumirán, seis (6) meses después de la entrada en vigencia de la presente ley, las funciones aquí establecidas. Para tales efectos, dentro de dicho término el Gobierno Nacional adoptará las medidas necesarias para adecuar la estructura de la Superintendencia de Industria, Comercio y Financiera dotándola de la capacidad presupuestal y técnica necesaria para cumplir con dichas funciones.

TITULO VII

DE LAS DISPOSICIONES FINALES

Artículo 21. *Régimen de transición*. Para el cumplimiento de las disposiciones contenidas en la presente ley, las personas que, a la fecha de su entrada en vigencia ejerzan alguna de las actividades aquí reguladas, tendrán un plazo de hasta seis (6) meses para adecuar su funcionamiento a las disposiciones de la presente ley.

Los titulares de la información que a la entrada en vigencia de esta ley estuvieren al día en sus obligaciones objeto de reporte, y cuya información negativa hubiere permanecido en los bancos de datos por lo menos un año contado a partir de la cancelación de las obligaciones, serán beneficiarios de la caducidad inmediata de la información negativa.

A su vez, los titulares de la información que se encuentren al día en sus obligaciones objeto de reporte, pero cuya información negativa no hubiere permanecido en los bancos de datos al menos un año después de canceladas las obligaciones, permanecerán con dicha información negativa por el tiempo que les hiciere falta para cumplir el año, contado a partir de la cancelación de las obligaciones.

Los titulares de la información que cancelen sus obligaciones objeto de reporte dentro de los seis (6) meses siguientes a la entrada en vigencia de la presente ley, permanecerán con dicha información negativa en los bancos de datos por el término de un (1) año, contado a partir de la fecha de cancelación de tales obligaciones. Cumplido este plazo de un (1) año, el dato negativo deberá ser retirado automáticamente de los bancos de datos.

El beneficio previsto en este artículo se perderá en caso que el titular de la información incurra nuevamente en mora, evento en el cual su reporte reflejará nuevamente la totalidad de los incumplimientos pasados, en los términos previstos en el artículo 13 de esta ley.

Artículo 22. *Vigencia y derogatorias*. Esta ley rige a partir de la fecha de publicación y deroga las disposiciones que le sean contrarias.

El Presidente del honorable Senado de la República,

Hernán Francisco Andrade Serrano.

El Secretario General del honorable Senado de la República,

Emilio Ramón Otero Dajud.

El Presidente de la honorable Cámara de Representantes,

Germán Varón Cotrino.

El Secretario General de la honorable Cámara de Representantes,

Jesús Alfonso Rodríguez Camargo.

REPUBLICA DE COLOMBIA - GOBIERNO NACIONAL

Publíquese y cúmplase.

Dada en Bogotá, D. C., a 31 de diciembre de 2008.

ÁLVARO URIBE VÉLEZ

El Director del Departamento Administrativo de la Presidencia de la República, Encargado de las funciones del Despacho del Ministro del Interior y de Justicia,

Bernardo Moreno Villegas

NOTA DE PIE DE PÁGINA:

1 Revisión Previa de Constitucionalidad. Declarado Exequible mediante Sentencia C- 1011 del 16 de octubre de 2008.

NOTA: Publicada en el Diario Oficial 47.219 de diciembre 31 de 2008

2.2.8 Ciberseguridad. Definido por ISACA (Information Systems Audit and Control Association – Asociación de Auditoría y Control sobre los Sistemas de Información) como "Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados".

Para el Ph. D Kevin Newmeyer, no existe consenso internacional en lo que constituye Ciberseguridad, lo entiende como el conjunto de prácticas políticas, de entrenamiento y tecnología, diseñada para proteger el entorno cibernético con la finalidad de asegurar la integridad de la información y habilidad de conectar dispositivos para que operen según diseño[12].

2.2.9 Ciberdefensa. El ministerio de asuntos exteriores y de cooperación de España en su estrategia de Seguridad Nacional la define como el instrumento necesario para proteger la seguridad en internet de los usuarios, los Estados, las empresas…. También indica que hay unas medidas mínimas como son el fomentar la cooperación internacional, mejorar las tecnologías de autenticación, divulgar campañas educativas con fin de protegerse en el mundo online y sensibilizar sobre el consumo digital seguro.[13]

[12] NEWMEYER. Kevin. Ciberespacio, ciberseguridad y ciberguerra. II simposio Internacional de Seguridad y Defensa Perú. 2015 publicaciones ESUP. Pag. 95

[13] MINISTERIO DE ASUNTOS EXTERIORES DE ESPAÑA. Ciberseguridad un desafío Internacional. 2017.

2.2.9.1 Grupos de respuesta a incidentes informáticos. En Colombia al igual que en muchos otros países, existen los grupos de respuesta a incidentes entre los cuales están:

1. **CSIRT-PONAL**. Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional Grupo creado para atender las necesidades de prevención, atención e investigación de los eventos e incidentes de seguridad informática, con el fin de proteger la infraestructura tecnológica, los activos de información y mitigar el impacto ocasionado por la materialización de los riesgos asociados con el uso de las tecnologías de la información y las telecomunicaciones.
2. **ColCERT** Grupo de Respuesta a Emergencias Cibernéticas de Colombia. A través de la Política Nacional de Ciberseguridad y Ciberdefensa Nacional, tiene como objetivo la coordinación de los temas de Ciberseguridad y Ciberdefensa y la protección de la Infraestructura Crítica Nacional.
3. **CCOC**. Comando Conjunto Cibernético de las Fuerzas Militares. Está en cabeza del Comando General de las Fuerzas Militares, quien podrá delegar sus funciones dentro de las Fuerzas Militares dependiendo de las especialidades existentes en el sector. Este deberá prevenir y contrarrestar toda amenaza o ataque de naturaleza cibernética que afecte los valores e intereses nacionales.

2.2.9.2 Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información en Colombia. Para el desarrollo de esta guía, se recogieron aspectos importantes de mejores prácticas y documentos de uso libre por parte del NIST (National Institute of Standards and Technology – (Computer Security Incident Handling Guide), tomando como base los lineamientos recomendados en Norma la ISO IEC 27001 – 2013 Numeral 16 de la misma, para la gestión de incidentes.

Esta guía de gestión de incidentes de seguridad de la información, plantea una serie de actividades para dar cumplimiento con el ciclo de vida de la gestión y respuesta a un incidente de seguridad, preparación, detección y análisis, contención erradicación y recuperación, y actividades Post-Incidente logrando llegar de nuevo a la preparación.

Para definir las actividades de esta guía se incorporaron componentes definidos por el NIST alineados con los requerimientos normativos de la NTC–ISO–IEC 27035-2013 para la estrategia de Gobierno en Línea.

Es recomendable que las entidades creen un equipo de atención de incidentes de seguridad en cómputo CSIRT (Computer Security Incident Response Team, Equipo de Respuesta ante Incidencias de Seguridad) o un grupo que haga sus veces, quienes se encargaran de definir los procedimientos a la atención de incidentes,

realizar la atención, manejar las relaciones con entes internos y externos, definir la clasificación de incidentes, y además de esto se encargaran de:

- Detección de Incidentes de Seguridad: Monitorear y verificar los elementos de control con el fin de detectar un posible incidente de seguridad de la información.
- Atención de Incidentes de Seguridad: Recibe y resuelve los incidentes de seguridad de acuerdo con los procedimientos establecidos.
- Recolección y Análisis de Evidencia Digital: Toma, preservación, documentación y análisis de evidencia cuando sea requerida.
- Anuncios de Seguridad: Deben mantener informados a los funcionarios, contratistas o terceros sobre las nuevas vulnerabilidades, actualizaciones a las plataformas y recomendaciones de seguridad informática a través de algún medio de comunicación (Web, Intranet, Correo).
- Auditoria y trazabilidad de Seguridad Informática: El equipo debe realizar verificaciones periódicas del estado de la plataforma para analizar nuevas vulnerabilidades y brechas de seguridad.
- Certificación de productos: El equipo verifica la implementación de las nuevas aplicaciones en producción para que se ajusten a los requerimientos de seguridad informática definidos por el equipo.
- Configuración y Administración de Dispositivos de Seguridad Informática: Se encargarán de la administración adecuada de los elementos de seguridad informática.
- Clasificación y priorización de servicios expuestos: Identificación de servicios sensibles y aplicaciones expuestas para la prevención o remediación de ataques.
- Investigación y Desarrollo: Deben realizar la búsqueda constante de nuevos productos en el mercado o desarrollo de nuevas herramientas de protección para combatir brechas de seguridad, y la proposición de nuevos proyectos de seguridad de la información.

Este grupo está enfocado principalmente en atender los incidentes de seguridad de la información que se presentan sobre los activos soportados por la plataforma tecnológica de la entidad.

PREPARACIÓN

Esta etapa dentro del ciclo de vida de respuesta a incidentes, suele hacerse pensando no sólo en crear un modelo que permita a la entidad estar en capacidad de responder ante estos, sino también en la forma como pueden ser detectados, evaluados y gestionar las vulnerabilidades para prevenirse, asegurando que los sistemas, redes, y aplicaciones son lo suficientemente seguros.

Aunque el equipo de respuesta a incidentes no es normalmente responsable de la prevención de incidentes, es muy importante que se considere como un componente fundamental de los programas de respuesta. Además, El equipo de respuesta a incidentes debe actuar como una herramienta de experiencia en el establecimiento de recomendaciones para el aseguramiento de los sistemas de información y la plataforma que los soporta.

En esta etapa el grupo de gestión de incidentes o quien se designe para esta labor, debe velar por la disposición de los recursos de atención de incidentes y las herramientas necesarias para cubrir las demás etapas del ciclo de vida del mismo, creando (si no existen) y validando (si existen) los procedimientos necesarios y programas de capacitación.

La etapa de preparación debe ser apoyada por la dirección de tecnologías de la información o quien haga sus veces, incluyendo las mejores prácticas para el aseguramiento de redes, sistemas, y aplicaciones, por ejemplo:

- Gestión de Parches de Seguridad: las entidades dependiendo de su estratificación deben contar con un programa de gestión de vulnerabilidades (Sistemas Operativos, Bases de Datos, Aplicaciones, Otro Software Instalado), este programa ayudara a los administradores en la identificación, adquisición, prueba e instalación de los parches.
- Aseguramiento de plataforma: las entidades dependiendo de si estratificación deben ser aseguradas correctamente. Se debe configurar la menor cantidad de servicios (principio de menor privilegio) con el fin de proveer únicamente aquellos servicios necesarios tanto a usuarios como a otros equipos. Se deben revisar configuraciones por default (usuarios, contraseñas y archivos compartidos). Cada recurso que pueda ser accedido por externos e incluso por usuarios internos debe desplegar alguna advertencia. Los servidores deben tener habilitados sus sistemas de auditoría para permitir el login de eventos.
- Seguridad en redes: Debe existir una gestión constante sobre los elementos de seguridad. Las reglas configuradas en equipos de seguridad como firewalls deben ser revisadas continuamente. Las firmas y actualizaciones de dispositivos como IDS o IPS deben encontrarse al día. Todos los elementos de seguridad y de red deben encontrarse sincronizados y sus logs deben ser enviados a un equipo centralizado de recolección de logs para su respectivo análisis.
- Prevención de código malicioso: Todos los equipos de la infraestructura (servidores como equipos de usuario) deben tener activo su antivirus, antimalware con las firmas de actualización al día.
- Sensibilización y entrenamiento de usuarios: Usuarios en la entidad incluidos los administradores de TI deben ser sensibilizados de acuerdo a las políticas y procedimientos existentes relacionados con el uso apropiado de redes,

sistemas y aplicaciones en concordancia con los estándares de seguridad de la entidad. Los encargados de los sistemas de información deben establecer las necesidades de capacitación de las personas encargadas de la protección de los datos.

Las actividades descritas anteriormente buscan prevenir la ocurrencia de incidentes de seguridad de la información que esta soportada por TI, y adicionalmente es necesario realizar una evaluación mensual.

RECURSOS DE COMUNICACIÓN

En este numeral se pretende enunciar los elementos necesarios para la comunicación del equipo de atención de incidentes dentro de la entidad.

Información de Contacto: Se debe tener una lista de información de contacto de cada una de las personas que conforman el grupo de gestión de incidentes o quienes realicen sus funciones.

- Información de Escalamiento: Se debe contar con información de contacto para el escalamiento de incidentes según la estructura de la entidad.
- Información de los administradores de la plataforma tecnológica (Servicios, Servidores)
- Contacto con el área de recursos humanos o quien realice sus funciones (por si se realizan acciones disciplinarias).
- Contacto con áreas interesadas o grupos de interés (CCP - Policía Nacional, Fiscalía, entre otras)

Política de Comunicación: La entidad debe tener una política de comunicación de los incidentes de seguridad para definir que incidente puede ser comunicado a los medios y cual no.

HARDWARE Y SOFTWARE

Para una correcta y eficiente gestión de incidentes la entidad debería tener en cuenta los siguientes elementos:

- Portátiles Forenses:
- Analizadores de protocolos.
- Software de adquisición.
- Software para recolección de evidencia.
- Kit de respuesta a incidentes.
- Software de análisis forense.
- Medios de almacenamiento

RECURSOS PARA EL ANÁLISIS DE INCIDENTES

- Tener un listado de los puertos conocidos y de los puertos utilizados para realizar un ataque.
- Tener un diagrama de red para tener la ubicación rápida de los recursos existentes
- Una Línea – Base de Información de: Servidores (Nombre, IP, Aplicaciones, Parches, Usuarios Configurados, responsable de cambios). Esta información siempre debe estar actualizada para poder conocer el funcionamiento normal del mismo y realizar una identificación más acertada de un incidente.
- Se debe tener un análisis del comportamiento de red estándar en este es recomendable incluir: puertos utilizados por los protocolos de red, horarios de utilización, direcciones IP con que generan un mayor tráfico, direcciones IP que reciben mayor número de peticiones.

RECURSOS PARA LA MITIGACIÓN Y REMEDIACIÓN

En este punto se consideran los elementos básicos para la contención de un posible incidente, Backup de Información, imágenes de servidores, y cualquier información base que pueda recuperar el funcionamiento normal del sistema.

DETECCIÓN, EVALUACION Y ANÁLISIS

Detección Identificación y Gestión de Elementos Indicadores de un Incidente Los indicadores son los eventos que nos señalan que posiblemente un incidente ha ocurrido, generalmente algunos de estos elementos son:

- Alertas en sistemas de seguridad
- Caídas de servidores
- Reportes de usuarios
- Software antivirus dando informes
- Otros funcionamientos fuera de lo normal del sistema

La identificación y gestión de elementos que alertan sobre un incidente, nos proveen de información que puede alertarnos sobre la futura ocurrencia del mismo y preparar procedimientos para minimizar su impacto. Algunos de estos elementos pueden ser:

- Logs de servidores
- Logs de aplicaciones
- Logs de herramientas de seguridad
- Cualquier otra herramienta que permita la identificación de un incidente de seguridad

En la entidad debe existir un listado de fuentes generadoras de eventos que permitan la identificación de un incidente de seguridad de la información.

ANÁLISIS

Las actividades de análisis del incidente involucran otra serie de componentes, por lo que es recomendable tener en cuenta los siguientes:

- Tener conocimientos de las características normales a nivel de red y de los sistemas.
- Los administradores de TI deben tener conocimiento total sobre los comportamientos de la Infraestructura que están Administrando.
- Toda información que permita realizar análisis al incidente debe estar centralizada (Logs de servidores, redes, aplicaciones).
- Es importante efectuar correlación de eventos, ya que por medio de este proceso se pueden descubrir patrones de comportamiento anormal y poder identificar de manera más fácil la causa del incidente.
- Para un correcto análisis de un incidente debe existir una única fuente de tiempo (Sincronización de Relojes) ya que esto facilita la correlación de eventos y el análisis de información.
- Se debe mantener y usar una base de conocimiento con información relacionada sobre nuevas vulnerabilidades, información de los servicios habilitados, y experiencias con incidentes anteriores.
- Crear matrices de diagnóstico e información para los administradores menos experimentados.

EVALUACIÓN

Para realizar la evaluación de un incidente de seguridad se debe tener en cuenta los niveles de impacto con base en los insumos entregados por el análisis de riesgos y la clasificación de activos de información de la entidad. La severidad del incidente puede ser:

- Alto Impacto: El incidente de seguridad afecta a activos de información considerados de impacto catastrófico y mayor que influyen directamente a los objetivos misionales del Instituto. Se incluyen en esta categoría aquellos incidentes que afecten la reputación y el buen nombre o involucren aspectos legales. Estos incidentes deben tener respuesta inmediata.
- Medio Impacto: El incidente de seguridad afecta a activos de información considerados de impacto moderado que influyen directamente a los objetivos de un proceso determinado.
- Bajo Impacto: El incidente de seguridad afecta a activos de información considerados de impacto menor e insignificante, que no influyen en ningún

objetivo. Estos incidentes deben ser monitoreados con el fin de evitar un cambio en el impacto.

Clasificación de Incidentes de seguridad de la información

Algunos ejemplos de clasificación de incidentes podrían ser (esta clasificación está sujeta a cada entidad dependiendo de su infraestructura, de sus riesgos y criticidad de los activos.): La clasificación dada es solo un ejemplo):

- Acceso no autorizado: Es un incidente que involucra a una persona, sistema o código malicioso que obtiene acceso lógico o físico sin autorización adecuada del dueño a un sistema, aplicación, información o un activo de información.
- Modificación de recursos no autorizado: Un incidente que involucra a una persona, sistema o código malicioso que afecta la integridad de la información o de un sistema de procesamiento.
- Uso inapropiado de recursos: Un incidente que involucra a una persona que viola alguna política de uso de recursos.
- No disponibilidad de los recursos: Un incidente que involucra a una persona, sistema o código malicioso que impide el uso autorizado de un activo de información.
- Multicomponente: Un incidente que involucra más de una categoría anteriormente mencionada.
- Otros: Un incidente que no puede clasificarse en alguna de las categorías anteriores. Este tipo de incidentes debe monitorearse con el fin de identificar la necesidad de crear nuevas categorías.

Priorización de los Incidentes y tiempos de respuesta

Con el fin de permitir una atención adecuada a los incidentes (análisis, contención y erradicación) se debe determinar el nivel de prioridad del mismo, y de esta manera atenderlos adecuadamente según la necesidad.

A manera de ejemplo, se definen una serie de variables que podrán ser utilizadas para realzar la evaluación de los incidentes:

- Prioridad
- Criticidad de impacto
- Impacto Actual
- Impacto Futuro

Nivel de Prioridad: Depende del valor o importancia dentro de la entidad y del proceso que soporta el o los sistemas afectados.

Impacto Actual: Depende de la cantidad de daño que ha provocado el incidente en el momento de ser detectado.

Impacto Futuro: Depende de la cantidad de daño que pueda causar el incidente si no es contenido, ni erradicado.

Luego de tener definidas las variables se obtiene la prioridad mediante la siguiente formula:

Nivel Prioridad = (Impacto actual * 2,5) + (Impacto futuro * 2,5) + (Criticidad

del Sistema * 5)

Y los resultados obtenidos se deben compara con la siguiente tabla para determinar la prioridad de atención:

Tiempos de Respuesta

Para el caso de la atención de incidentes de seguridad se ha establecido unos tiempos máximos de atención de los mismos, con el fin de atender adecuadamente

los incidentes de acuerdo a su criticidad e impacto. Los tiempos expresados en la siguiente Tabla son un acercamiento al tiempo máximo en que el incidente debe ser atendido, y no al tiempo en el cual el incidente debe ser solucionado. Esto se debe a que la solución de los incidentes puede variar dependiendo del caso.

Cabe resaltar que cada entidad está en la libertad de definir tiempos de atención a incidentes como crean conveniente y dependiendo de la criticidad de los activos impactados.

Declaración y Notificación de Incidentes

Un incidente de seguridad de la información se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una Política de Seguridad de la Información de la entidad.

La notificación de los incidentes permite responder a los mismos en forma sistemática, minimizar su ocurrencia, facilitar una recuperación rápida y eficiente de las actividades minimizando la pérdida de información y la interrupción de los servicios, y el proceso de tratamiento de incidentes, y manejar correctamente los aspectos legales que pudieran surgir durante este proceso.

A continuación, se describe un proceso de notificación de incidentes de seguridad que podría ser adoptado por la entidad:

Un usuario, tercero o contratista que sospeche sobre la materialización de un incidente de seguridad deberá notificarlo al primer punto de contacto definido por la entidad (Ej: Soporte de primer nivel). El incidente puede ser notificado a través de cualquier canal de comunicación (Telefónico, Correo, Aplicativo) es importante resaltar que debe existir un formato el cual el usuario que reporta el incidente, debe

diligenciar con la mayor cantidad posible de información relacionada con el incidente.

El primer punto de contacto identificará el tipo de incidente (de acuerdo a la tabla de clasificación de incidentes que realiza la entidad). Analizará si el incidente reportado corresponde a un incidente de seguridad de la información o está relacionado con requerimientos propios de la infraestructura de TI. En caso de ser catalogado como un incidente de seguridad se notificarán a la persona encargada de la atención de incidentes o a quien haga sus veces para que tome las decisiones correspondientes. El primer punto de contacto será el encargado de realizar el seguimiento del Incidente hasta su cierre definitivo.

Si el incidente de seguridad es identificado por otra línea diferente a un usuario de la entidad, a través de los elementos de detección o administradores de TI, este es notificado directamente a la persona encargada de atención de incidentes quien tomará las acciones necesarias de atención. Se notificará al primer punto de contacto sobre la presentación de un incidente de seguridad para que realice la documentación respectiva y esté atento al seguimiento y desarrollo del mismo.

El punto de contacto clave dentro de la gestión de incidentes es la persona encargada de la atención de los mismos, el cual se encarga de coordinar y asignar las actividades con las partes interesadas. Estos últimos se encargan de solicitar el apoyo a las personas involucradas con el proceso con el fin de la correcta ejecución de actividades que den solución al incidente.

La persona encargada de la atención de incidentes tendrá la potestad para decidir sobre las acciones que se deban ejecutar ante la presencia de un incidente de seguridad y es la persona que notificará a las altas directivas de la entidad.

CONTENCIÓN ERRADICACIÓN Y RECUPERACIÓN

Es importante para la entidad implementar una estrategia que permita tomar decisiones oportunamente para evitar la propagación del incidente y así disminuir los daños a los recursos de TI y la pérdida de la confidencialidad, integridad y disponibilidad de la información.

Esta fase se descompone claramente en tres componentes:

Contención: esta actividad busca la detección del incidente con el fin de que no se propague y pueda generar más daños a la información o a la arquitectura de TI, para facilitar esta tarea la entidad debe poseer una estrategia de contención previamente definida para poder tomar decisiones, por ejemplo: apagar sistema, desconectar red, deshabilitar servicios.

La estrategia de contención varía según el tipo de incidente y los criterios deben estar bien documentados para facilitar la rápida y eficaz toma de decisiones.

Algunos criterios que pueden ser tomados como base son:

- Criterios Forenses
- Daño potencial y hurto de activos
- Necesidades para la preservación de evidencia
- Disponibilidad del servicio
- Tiempo y recursos para implementar la estrategia
- Efectividad de la estrategia para contener el incidente (parcial o total)
- Duración de la solución

Erradicación y Recuperación: Después de que el incidente ha sido contenido se debe realizar una erradicación y eliminación de cualquier rastro dejado por el incidente como código malicioso y posteriormente se procede a la recuperación a través de la restauración de los sistemas y/o servicios afectados para lo cual el administrador de TI o quien haga sus veces deben restablecer la funcionalidad de los sistemas afectados, y realizar un endurecimiento del sistema que permita prevenir incidentes similares en el futuro. En algunas ocasiones durante el proceso de Atención de Incidentes de Seguridad Informática específicamente en la fase de "Contención, Erradicación y Recuperación" se puede hacer necesario activar el BCP (Plan de Continuidad del Negocio) o el DRP (Plan de Recuperación de Desastres) en el caso que un incidente afecte gravemente a un determinado sistema.

ACTIVIDADES POST-INCIDENTE

Las actividades Post-Incidente básicamente se componen del reporte apropiado del Incidente, de la generación de lecciones aprendidas, del establecimiento de medidas tecnológicas, disciplinarias y penales de ser necesarias, así como el registro en la base de conocimiento para alimentar los indicadores.

Lecciones Aprendidas:

Una de las partes más importantes de un plan de respuesta a incidentes de TI es la de aprender y mejorar. Cada equipo de respuesta a incidentes debe evolucionar para reflejar las nuevas amenazas, la mejora de la tecnología, y las lecciones aprendidas. Mantener un proceso de "lecciones aprendidas" después de un incidente grave, y periódicamente después de los incidentes menores, es sumamente útil en la mejora de las medidas de seguridad y el proceso de gestión de incidentes

Mantener un adecuado registro de lecciones aprendidas permite conocer:

- Exactamente lo que sucedió, en qué momento y cómo el personal gestionó el incidente.
- Los procedimientos documentados.
- Si se tomaron las medidas o acciones que podrían haber impedido la recuperación.

- Cuál sería la gestión de personal y que debería hacerse la próxima vez que ocurra un incidente similar.
- Acciones correctivas pueden prevenir incidentes similares en el futuro.
- Cuales herramientas o recursos adicionales son necesarios para detectar, analizar y mitigar los incidentes en el futuro.

El proceso de lecciones aprendidas puede poner de manifiesto la falta de un paso o una inexactitud en un procedimiento y son un punto de partida para el cambio, y es precisamente debido a la naturaleza cambiante de la tecnología de la información y los cambios en el personal, que el equipo de respuesta a incidentes debe revisar toda la documentación y los procedimientos para el manejo de incidentes en determinados intervalos.

ROLES Y PERFILES NECESARIOS PARA LA ATENCIÓN DE INCIDENTES

A continuación, presentaremos una descripción de los actores que intervienen y conforman el proceso de atención de Incidentes, para cada actor se presentará una breve descripción sobre su perfil y la función dentro del proceso de respuesta a Incidentes de Seguridad de la información.

Usuario Sensibilizado: Es un empleado, empleados de firmas contratista o terceros con acceso a la infraestructura de la entidad, quien debe estar educado y concientizado sobre las guías implementadas sobre la seguridad de la información y en particular la guía de atención de incidentes, estos usuarios serán muchas veces quienes reporten los problemas y deberán tener en cuenta lo siguiente: Agente Primer Punto de Contacto: Es el encargado de recibir las solicitudes por parte de los usuarios sobre posibles incidentes también debe registrarlos en la base de conocimiento y debe ser el encargado de escalarlos a la persona encargada de la atención de incidentes. Este Agente debe contar adicionalmente con capacitación en Seguridad de la Información (con un componente tecnológico fuerte) y debe conocer perfectamente la clasificación de Incidentes y los procesos de escalamiento de Incidentes. Adicionalmente debe contar con una capacitación básica en técnicas forenses, específicamente en recolección y manejo de evidencia, lo cual involucra fundamentalmente dos aspectos.

- Admisibilidad de la evidencia: si la evidencia se puede utilizar o no en una corte
- Peso de la evidencia: la calidad y cabalidad de la evidencia.

Este no es un actor que realiza la centralización de los incidentes reportados por los usuarios, da un tratamiento inicial y escala el incidente para que sea tratado.

Administrador del Sistema. Se define como la persona encargada para configurar y mantener un activo informático. También debe ser notificado por el agente de primer punto de contacto sobre un incidente de seguridad con el fin de analizar,

identificar, contener y erradicar un incidente de seguridad. Este debe documentar y notificar al agente de primer punto de contacto sobre el incidente la solución del mismo. Se recomienda que los administradores cuenten con capacitación en Seguridad de la Información (con un componente tecnológico fuerte no solo en su plataforma si no en Redes y erradicación de vulnerabilidades) y debe conocer perfectamente la clasificación de Incidentes y los procesos de escalamiento de Incidentes. Adicionalmente debe contar con una capacitación en técnicas forenses, específicamente en recolección y manejo de evidencia.

Administrador de los sistemas de Seguridad. Personas encargadas de configurar y mantener un activo informático relacionado con la seguridad de la plataforma ej. Firewall, Sistemas de Prevención de Intrusos, Routers, Sistemas de Gestión y Monitoreo. También debe ser notificado por el agente de primero contacto sobre un incidente de seguridad con el fin de analizar, identificar, contener y erradicar un incidente de seguridad. Este debe documentar y notificar al agente de primer contacto sobre el incidente y la solución del mismo. Se recomienda que los administradores de esta tecnología sean expertos en Seguridad de la Información (con un componente tecnológico fuerte en Redes y erradicación de vulnerabilidades, Ethical Hacking y técnicas forenses) y debe conocer perfectamente la clasificación de Incidentes de la entidad.

Analista Forense. Es un experto en el tema forense, quien debe estar disponible en caso de que un incidente de impacto alto (o uno que amerite acciones disciplinarias o legales o investigación profunda) requiera una investigación completa para solucionarlo y determinar los siguientes Ítems

- Que sucedió.
- Donde sucedió.
- Cuando Sucedió.
- Quien fue el responsable.
- Como sucedió.

Este actor debe ser un apoyo para los demás actores en caso de dudas sobre los procedimientos y debe ejercer un liderazgo técnico en el proceso de atención de Incidentes de seguridad de la información.

Líder del Grupo de Atención de Incidentes. Responde a las consultas sobre los incidentes de seguridad que impacten de forma inmediata, y es el encargado de revisar y evaluar los indicadores de gestión correspondientes a la atención de incidentes de seguridad para poder ser presentados a los directivos. El Líder Grupo de Atención de Incidentes estará en la capacidad de convocar la participación de otros funcionarios de la organización cuando el incidente lo amerita (Prensa y Comunicaciones, Gestión de Talento Humano, Gestión Jurídica, Tecnología, Representante de las Directivas para el SGSI). También debe estar al tanto del cumplimiento de los perfiles mencionados y de revisar el cumplimiento de los procedimientos y mejores prácticas, así como también de los indicadores de gestión, y en capacidad de disparar si lo amerita planes de contingencia y/o

continuidad. Finalmente, el Líder del Grupo de Atención de Incidentes será el responsable del modelo de Gestión de incidentes y debe estar en la capacidad de revisar todos los incidentes de seguridad y los aspectos contractuales que manejan el outsourcing del servicio help desk.

RECOMENDACIONES FINALES Y A QUIÉN DEBO INFORMAR

1. Verificar la existencia y disponibilidad del levantamiento de información, relativa a los servicios de soporte de la infraestructura tecnológica de la entidad, incluyendo contactos de proveedores de servicios de alojamiento (hosting), gestión de contenidos en línea, disponibilidad de personal de soporte técnico, encargados de tecnología y seguridad informática, con el fin de garantizar un oportuno contacto en caso de incidentes.

2. Coordinar con los responsables de soporte técnico, que éstos hayan ejecutado o ejecuten con prontitud, todas las acciones que se requieran para asegurar y fortalecer los componentes de tecnologías de la información mencionados en la etapa de preparación. Dichas acciones contemplan verificación de usuarios y claves de acceso, actualizaciones de sistemas operativos y software de plataformas de servicios de base y gestión de contenidos, entre otros. Cualquier ejercicio de auditoria o verificación del cumplimiento de este tipo de actividades será de mucha utilidad.

3. Actualizar todos los datos de contacto relativos al nombre de dominio de la entidad, de tal forma que queden reflejados en el servicio público de información de registros de nombres de dominio WHOIS.CO. Esta información es de suma importancia para contactar a la entidad, en caso de presentarse un incidente. Cabe aclarar que, según lo indicado en el artículo 5 de la Resolución 1652 del 2008, cuando el Registrante o titular de un nombre de dominio bajo ".CO" suministre información "falsa, incorrecta o inexacta", el nombre de dominio podrá ser suspendido e incluso dado de baja. Si se requiere información para realizar dicha actividad de actualización, favor ingresar a la página http://www.cointernet.com.co/panel-de-control o comunicarse al siguiente número telefónico en Bogotá 6169961.

4. En el evento de que algún componente de la infraestructura tecnológica (sitios Web, aplicaciones, servicios en línea, sistemas de información, entre otros) de la Entidad, haya sido vulnerado o comprometido, reportar en primera instancia al ColCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia) por medio de correo electrónico a:contacto@colcert.gov.co o al Teléfono: (+571) 2959897.

En SEGUNDA instancia, adoptar las medidas y acciones necesarias para mitigar y resolver el incidente con el apoyo del personal encargado de la gestión de incidentes de la entidad, teniendo en cuenta la relevancia de ejecutar todos los procedimientos técnicos y operativos que faciliten la conservación (preservación) de las evidencias

de naturaleza digital y soportes del incidente, fundamentales para tramitar su posterior judicialización ante la autoridad competente.

5. Cuando se tenga evidencia de un incidente informático, la entidad afectada se pondrá en contacto con el Cai Virtual de la Policía Nacional www.ccp.gov.co, Centro Cibernético Policial de la Policía Nacional al teléfono 4266900 ext. 104092, para recibir asesoría del caso en particular y posterior judicialización. Es importante aclarar que solamente, en caso de lograrse un contacto exitoso, y tras establecerse de común acuerdo que el incidente pone en riesgo la estabilidad, seguridad y resiliencia del sistema de nombres de dominio, así como de otras entidades involucradas en el hecho, e incluso la reputación de la entidad, el responsable de la misma podrá solicitar, a través de un correo electrónico, se suspenda temporalmente el nombre de dominio mientras se gestiona internamente el incidente. Para el efecto, la comunicación deberá ser remitida desde cualquiera de las direcciones registradas en el WHOIS con destino al CCP de la Policía Nacional indicando motivo/situación detallada de afectación y solicitando de manera expresa asumiendo plena/total responsabilidad por las consecuencias técnicas/operacionales (sistema de correo, aplicaciones en línea bajo el dominio, etc.) de dicha acción solicitada.

Dicho mensaje deberá incluir la información de contacto telefónico del remitente para realizar su respectiva validación y proceder de conformidad[14].

2.2.9.3 Seguridad física. Es de suma importancia, tanto a nivel de empresa como personal, comprende factores de riesgo como el espacio, la humedad, luz solar, temperatura, partículas de polvo, campos magnéticos, suelos, vibraciones y golpes.

Luego, se puede definir la seguridad física como el conjunto de medidas de prevención y detección destinadas a evitar los daños físicos a los sistemas informáticos y proteger los datos almacenados en ellos.

Los riesgos externos a los que están sujetos los sistemas informáticos y las medidas preventivas que se pueden adoptar son los siguientes:

- ✓ Fenómenos naturales, como inundaciones, tormentas, terremotos, etc. Se pueden adoptar medidas preventivas como la instalación de los equipos en ubicaciones adecuadas dotadas de las oportunas medidas de protección (ubicaciones seguras, pararrayos, etc.).

[14] MINTIC, Ministerio de Tecnologías, Información y Comunicaciones. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. 2016 [citado 2017-10-10]. Disponible en internet <https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf>.

- ✓ Riesgos humanos, como actos involuntarios, actos vandálicos y sabotajes. Entre las medidas preventivas estarían: control de acceso a recintos, elaboración de perfiles psicológicos de empleados con acceso a datos.

2.2.9.4 Seguridad lógica. Es el conjunto de medidas destinadas a la protección de los datos y aplicaciones informáticas, así como a garantizar el acceso a la información únicamente por las personas autorizadas. Algunas de las medidas o mecanismos establecidos en las políticas de seguridad son las siguientes:

- ➢ Autenticación de usuarios: sistema que trata de evitar accesos indebidos a la información a través de un proceso de identificación de usuarios, que en muchos casos se realiza mediante un nombre de usuario y una contraseña.
- ➢ Listas de control de acceso: mecanismos que controlan qué usuarios, roles o grupos de usuarios pueden realizar qué cosas sobre los recursos del sistema operativo.
- ➢ Criptografía: técnica que consiste en transformar un mensaje comprensible en otro cifrado según algún algoritmo complejo para evitar que personas no autorizadas accedan o modifiquen la información.
- ➢ Certificados digitales: documentos digitales, identificados por un número de serie único y con un periodo de validez incluido en el propio certificado, mediante los cuales una autoridad de certificación acredita la identidad de su propietario vinculándolo con una clave pública.
- ➢ Firmas digitales: es el conjunto de datos, en forma electrónica, consignados junto a otros o asociados con ellos que pueden ser utilizados como medio de identificación del firmante. Ejemplo: DNI electrónico.
- ➢ Cifrado de unidades de disco o sistemas de archivos: medidas que protegen la confidencialidad de la información. Además, en las políticas, como en todos los reglamentos, no solo se establecen obligaciones y protocolos de actuación, sino que también se pueden establecer sanciones para el caso de incumplimiento de sus disposiciones.

Zona Desmilitarizada DMZ, Delimitarrized Zone, también conocida como screened subnet, es un segmento de la red de la organización que se encuentra en una zona perimetral, en el cual se van a ubicar los servidores que pueden ser accesibles desde el exterior. Se trata de una red planteada como una zona intermedia que permite mejorar el aislamiento entre la parte pública y la parte privada de la red de una organización. En la práctica, se suelen utilizar dos routers para definir la zona DMZ, uno exterior y otro interior, así como un cortafuegos con tres tarjetas de red (tri-homed bastion host), aunque también se podría recurrir a una configuración que utilice varios cortafuegos.

Por este motivo, se recomienda separar los servicios internos de los ofrecidos a usuarios externos, tratando de evitar que en un mismo equipo se puedan instalar ambos tipos de servicios. Así mismo, convendría emplear direcciones IP privadas para todos los servidores que se encuentran en la parte interna de la red de la organización. También se podría ubicar un servidor proxy o un gateway dentro de la zona DMZ, que actúe como pasarela de aplicación para algunos servicios ofrecidos a los usuarios internos. En la práctica, en redes de ordenadores de una cierta complejidad es necesario utilizar varios cortafuegos para reforzar la seguridad, aplicando el principio de "defensa en profundidad", disponiendo de varios niveles o barreras de protección frente a los intrusos. También se recurre a la utilización de lo que se ha denominado como "zona muerta" (Dead Zone), que consiste en un segmento de red intercalado entre dos routers en el que se utiliza un protocolo distinto a TCP/IP (como podría ser IPX o NetBEUI), para impedir que un intruso que se conecte desde Internet pueda atravesar dicho segmento y acceder a la parte más interna de la red de una organización. Para su implantación es necesario recurrir a técnicas de conversión de protocolos, realizadas por los propios routers que delimitan la "zona muerta"[15].

2.3 MARCO CONCEPTUAL

2.3.1 Cibercrimen. Delito económico, como el fraude informático, el robo, la falsificación, el hacking, el espionaje informático, el sabotaje, la extorsión informática, la piratería comercial y otros crímenes contra la propiedad intelectual, la invasión de la intimidad, la distribución de contenidos ilegales y dañosos, la incitación a la prostitución y otras actitudes que atenten contra la moralidad, y el crimen organizado. [16]

2.3.2 Ciberterrorismo. Es la convergencia del ciberespacio y el terrorismo, es decir, "la forma en la que el terrorismo utiliza las tecnologías de la información para intimidar, coaccionar o para causar daños a grupos sociales con fines políticos-religiosos". Cambia las armas, las bombas y los misiles por una computadora para planificar y ejecutar unos ataques que produzcan los mayores daños posibles a la población civil. [17]

2.3.3 Ciberdelincuencia. Comprende cualquier acto criminal que utilice ordenadores y redes. Además, la ciberdelincuencia también incluye delitos tradicionales realizados a través de Internet. Por ejemplo: los delitos motivados por

[15] GOMEZ. Álvaro. Auditoría de seguridad informática. Madrid, ES: RA-MA Editorial, 2014.
[16] MEDERO, Gema. Ciberespacio y el crimen organizado. 2012. Revista Enfoques. Pág. 20
[17] MEDERO, Gema. Ciberespacio y el crimen organizado. 2012. Revista Enfoques. Pág. 20

prejuicios, el telemarketing y fraude de Internet, la suplantación de identidad y el robo de cuentas de tarjetas de crédito se consideran ciberdelitos cuando las actividades ilegales se llevan a cabo utilizando un ordenador e Internet[18] citado por Emilio Florez[19]

2.3.4 Ciberespacio. Citado por Luis Recalde[20] El Departamento de Defensa de Estados Unidos precisa que: "El ciberespacio es un ámbito operativo cuyo carácter distintivo y único está enmarcada por el uso de la electrónica y el espectro electromagnético para crear, almacenar, modificar, intercambiar y explotar la información a través de las tecnologías de información y comunicación (TIC) y basadas en sistemas interconectados con sus infraestructuras asociadas" [21]

Gibson en Neuromancer, define ciberespacio, como alucinación consensual experimentada diariamente operada por billones de operadores autorizados en cada nación, por niños que aprenden conceptos matemáticos…. Una representación gráfica de datos abstraídos de las memorias de cada computador en el sistema humano. Complejidad impensable. Líneas de luz que vagan en el no lugar de la mente, agrupaciones y constelaciones de datos. Como las luces de la ciudad retrocediendo…[22]. El ciberespacio ha servido de infraestructura para la globalización al tomar como proceso de globalización un conjunto de flujos no-iso mórficos de personas, tecnologías, finanzas, imágenes, información e ideas[23] citado por Vanessa Fonseca[24]

2.4. MARCO LEGAL

En cuanto a legislación se refiere, es de aclarar que el Convenio de ciberdelincuencia da unas pautas o guía para que cada país legisle de forma integral y acorde a sus preceptos dentro de lo que su constitución o carta magna les permita, de forma que pueda llegar a ser vinculante a un marco de cooperación internacional, ya sea como estado adherido o como parte del mismo convenio.

---

[18] NORTON. Informe de Cibercrimen. 2011

[19] FLOREZ. Emilio. Ciberdelincuencia un mal que afecta a la sociedad actual. 2014. [en línea]. <http://www.egov.ufsc.br/portal/sites/default/files/ciberdelincuencia_un_mal_que_afecta_a_la_sociedad_actual.pdf > [citado en 15 de octubre 2017]

[20] RECALDE. Luis. El Ciberespacio: El Nuevo mundo de guerra global. Revista de Ciencias de Seguridad y Defensa Vol. 1, No. 2, 2016.

[21] KUELH. Dan. Cyberspace to Cyberpower: Defining the Problem, Information Resources Management. 2006. The National Military Strategy for Cyberspace Operations, Washington

[22] GIBSON. William. Neuromancer. New York. 1984 Pag. 51

[23] FEATHERSTONE. Mike. Undoing Culture. Globalization, Posmodernism and Identity. London. 1995 Pag. 153

[24] FONSECA. Vanessa. Ciberespacio: reinventando, la metáfora de lo humano. Revista Bibliotecas. Vol. 21, No. 1-2, 2003. San José, CR: Red Universidad Nacional de Costa Rica, 2003.

2.4.1 Convenio de ciberdelincuencia. El convenio de ciberdelincuencia de Budapest, está enmarcado dentro de los convenios celebrados dentro del consejo de Europa, es un tratado de carácter internacional, por tal razón está cubierto por todos los derechos de los tratados de la convención de Viena de 1969.

En el caso del tratado de ciberdelincuencia de Budapest se aplica:

"Los convenios del Consejo de Europa no son actos reglamentarios de la Organización. Ellos deben su existencia legal para el consentimiento de los Estados miembros que firmen y ratifiquen.

Por otra parte, la gran mayoría de los convenios del Consejo de Europa exigen a los Estados no miembros de la Organización para convertirse en Partes del mismo, ser invitados por el Comité de Ministros del Consejo de Europa y por medio del procedimiento de adhesión.

El Secretario General es el depositario de los convenios del Consejo de Europa. Él es el guardián de estas convenciones y preside la firma y el depósito de los instrumentos de ratificación, aceptación, aprobación o adhesión. Es también el secretario general, el responsable de las notificaciones previstas en las disposiciones finales de los convenios, y su registro en la Secretaría de las Naciones Unidas".[25].

2.4.2 Legislación Colombiana en Seguridad Informática. Colombia es un País que bien se podría decir ha modificado y legislado de forma paulatina y coordinada en materia de seguridad informática, actualmente cuenta con:

Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.[26]

Ley 599 de 2000. Por la cual se expide el Código Penal Colombiano. En esta se mantuvo la estructura del tipo penal de "violación ilícita de comunicaciones", se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento,

---

[25]PORTAL COUNCIL OF EUROPE. Acerca de los tratados [en línea]. <http://www.coe.int/en/web/conventions/about-treaties> [citado en 5 de octubre 2016]

[26] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 527 de 1999. (18, agosto, 1999). por la cual se definen y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación. [en línea]. <http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/LEY_527_DE_1999.pdf> [citado en 7 de octubre 2016]

venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Se tipificó el “Acceso abusivo a un sistema informático” [27]

Decreto 1524 de 2002. Por el cual reglamenta el artículo 5o. de la Ley 679 de 2001 referente a Pornografía en menores de edad.[28]

Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.[29]

Ley 1341 de 2009. Define principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la Información y las Comunicaciones –TIC, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones. [30]

Ley 1336 de 2009. Por la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes. [31]

Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de

---

[27]COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 599 de 2000. (24, julio, 2000). por la cual se Expide el Código Penal. En esta se mantuvo la estructura del tipo penal de “violación ilícita de comunicaciones”, se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. [en línea]. <http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html> [citado en 7 de noviembre 2016]

[28] COLOMBIA, MINISTERIO DE COMUNICACIONES. Decreto 1524 de 2002. (30, julio, 2002). El cual reglamenta el artículo 5o. de la Ley 679 de 2001 referente a Pornografía en menores de edad. [en línea]. <http://www.icbf.gov.co/cargues/avance/docs/decreto_1524_2002.htm> [citado en 7 de noviembre 2016]

[29] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley Estatutaria 1266. (31, diciembre, 2008). Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países. [en línea]. <https://www.bancoldex.com/documentos/1291_Ley_1266_de_2008_(Habeas_Data).pdf> [citado en 7 de noviembre 2016]

[30] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1341 de 2009. (30, julio, 2009). por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones - TIC-, se crea la agencia nacional del espectro y se dictan otras disposiciones. [en línea]. <http://www.mintic.gov.co/portal/604/articles-3707_documento.pdf> [citado en 7 de noviembre 2016]

[31] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1336 de 2009. (21, julio, 2009). por la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes. [en línea]. <http://www.anato.org/sites/default/files/Ley1336de2009.pdf> [citado en 17 de noviembre 2016]

los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.[32]

Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. [33]

Sin embargo, la situación en Colombia durante el año 2015 presento 7.118 denuncias, 40% más que en el 2014, un incremento en más del 50% en amenazas cibernéticas, 4.572 (64%) casos fueron hurtos por medios informáticos, 1.087 (15.27%) casos de abusos de sistemas informáticos en total generaron más de 600 millones de pesos en pérdidas durante el año 2015. [34]

[32]COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1273 de 2009. (05, enero, 2009). por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. [en línea]. <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492> [citado en 17 de noviembre 2016]

[33] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1581 de 2012. (17, octubre, 2012). por la cual se dictan disposiciones generales para la protección de datos personales. [en línea]. <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981> [citado en 7 de octubre 2016]

[34] MEDINA, Edgar. El tiempo. Tecnosfera, En 2015, cibercrimen generó pérdidas por US$ 600 millones en Colombia. [Online]. Colombia: 2015. [citado 2016-11-17]. Disponible en internet <http://www.eltiempo.com/tecnosfera/tutoriales-tecnologia/cuantos-delitos-informaticos-se-denuncian-en-colombia/16493604>.

3 DESARROLLO DEL PROYECTO

3.1 LOS PAÍSES ADHERIDOS

3.1.1 Canadá. Realizo firma del convenio el 23 de noviembre de 2001, entro en vigor el 1 de julio de 2004 y lo ratifico el 8 de julio de 2015, entrando de nuevo en vigor el 1 de noviembre de 2015, a pesar de haber firmado el convenio desde el inicio, solo lo ratifico hasta el año 2015, debido a las medidas legislativas que debía adoptar, en especial lo concerniente a la libertad civil y la privacidad.

Canadá comenzó a participar en las actividades del Consejo de Europa en la década de 1960, pero no como observador oficial con el Comité de Ministros. En 1997, se le concedió estatus oficial de observador en la Asamblea Parlamentaria del Consejo de Europa (al igual que México e Israel). Canadá también ha firmado y ayudado a desarrollar otros convenios del Consejo de Europa.[35]

En el año 2012, el 83% de los mayores de 16 años utilizaba Internet para uso personal, la banca en línea era el 72%, el uso de redes sociales 67%, a ordenar bienes y servicios en línea correspondía a un 56%, compras en línea 18,9 millones de dólares (Statistics Canadá 2013).[36]

En Canadá, la policía cubre el 80% de la población y se reportaron 9.084 casos de delitos informáticos en 2012, el más común fue el fraude con 54%, intimidación 20%, violación sexual 16%. El acusado fue identificado en el 6% de los delitos relacionados con la propiedad, el 31% en violaciones ciber-sexuales, y el 55% relacionados con violaciones de intimidación.[37]

En Canadá la policía posee una página dedicada exclusivamente a informar sobre datos estadísticos de ciberdelincuencia la cual puede ser consultada en

http://www.statcan.gc.ca/pub/85-002-x/2014001/article/14093-eng.htm

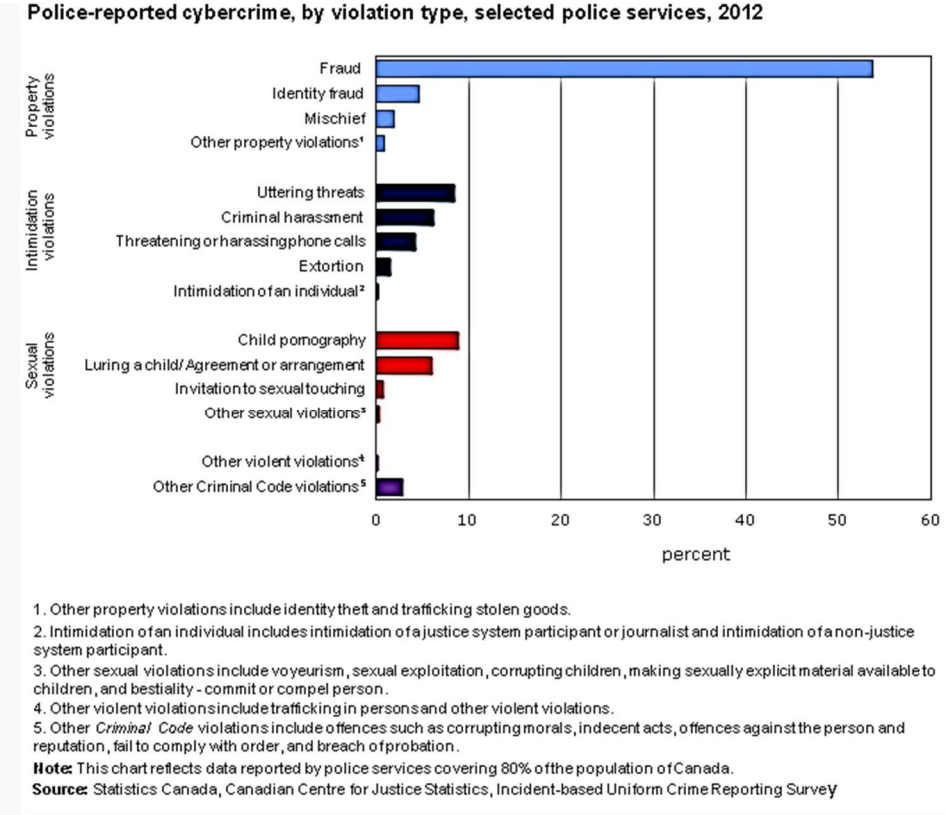
---

[35] CANADA, Government. Canada and the Council of Europe. [Online]. Canadá: 2015. [citado 2016-11-20]. Disponible en internet <http://www.canadainternational.gc.ca/eu-ue/bilateral_relations_bilaterales/council_europe_conseil.aspx?lang=eng>.

[36] CANADA, Statistics. Police-reported cybercrime in Canada, 2012. [Online]. Canadá: 2012. [citado 2016-11-20]. Disponible en internet <http://www.statcan.gc.ca/pub/85-002-x/2014001/article/14093-eng.htm>.

[37] CANADA. Op. Cit. Disponible en internet <http://www.statcan.gc.ca/pub/85-002-x/2014001/article/14093-eng.htm>.

Grafica 4 Reporte cibercrimen a 2012



Fuente 10 http://www.statcan.gc.ca/pub/85-002-x/2014001/article/14093-eng.htm

La ley en contra del delito informático se encuentra tipificada en el código penal en las secciones 184 (privacidad), 342 (robo, falsificación y uso no autorizado de equipo), 402 (robo de identidad), 403 (fraude de identidad), 490 (delincuentes sexuales de la información),[38]

3.1.2 República Dominicana. Al día de hoy no tiene ninguna estrategia nacional de seguridad cibernética, ni una política coordinada de defensa cibernética, a pesar de la participación de las agencias en la CICDAT (Comisión Interinstitucional contra

[38] CANADA, Government of. Justice Laws Website, Criminal Code (R.S.C., 1985, c. C-46). [Online]. Canadá: 2016. [citado 2016-11-20]. Disponible en internet <http://laws-lois.justice.gc.ca/eng/acts/c-46/index.html>.

Crímenes y Delitos de Alta Tecnología), el nivel de sensibilización sobre la seguridad cibernética dentro del gobierno es generalmente bajo.[39]

A febrero de 2016, los ciber-ataques afectaban sectores claves como el gobierno, cuerpos castrenses, financiero, educativo, salud, energético, comercio, industria, Mipymes. Los ciber-ataques en sus diversas modalidades se han convertido en un potente instrumento de agresión contra los ciudadanos, las instituciones públicas y las empresas causando grandes daños a nivel nacional e internacional.[40]

3.1.3 Australia. Ratifico el Convenio el 30 de noviembre de 2012, entrando en vigor el 1 de marzo de 2013. Los datos registrados corresponden a un país desarrollado, existen 1,61 computadoras por hogar en 2009 (Atlas Digital de Australia, 2009), el 14% de las empresas australianas experimentaron incidentes de ciberdelincuencia en 2006-07 (encuesta de evaluación del negocio Seguridad del usuario Australiana de Informática, 2009). Un estudio de la Universidad de Monash encontró que el 72% de los estudiantes de la escuela secundaria australianos encuestados había experimentado el contacto no deseado o desagradable por desconocidos en su perfil de red social.[41]

CERT es el organismo asociado al Centro de Seguridad Cibernética de Australia (ACSC) entre el año 2014 y 2015 respondió a 11.733 incidentes que afectaron a empresas (218 intervienen con sistemas de interés nacional y la infraestructura crítica).[42]

Como se puede constatar en la gráfica número 5, el CERT y la ASCS de Australia a través de una encuesta sobre incidentes ocurridos en el año anterior brindaron respuestas de que el 42% no había tenido incidentes, el 8% no sabía, el 40% había presentado entre 1 y 5, el 6% de las personas presentaron entre 6 y 10 incidentes y el 5% restante, más de 10 incidentes, lo cual es una cifra considerable al tener presente que es un país altamente desarrollado en lo que a tecnología se refiere.

---

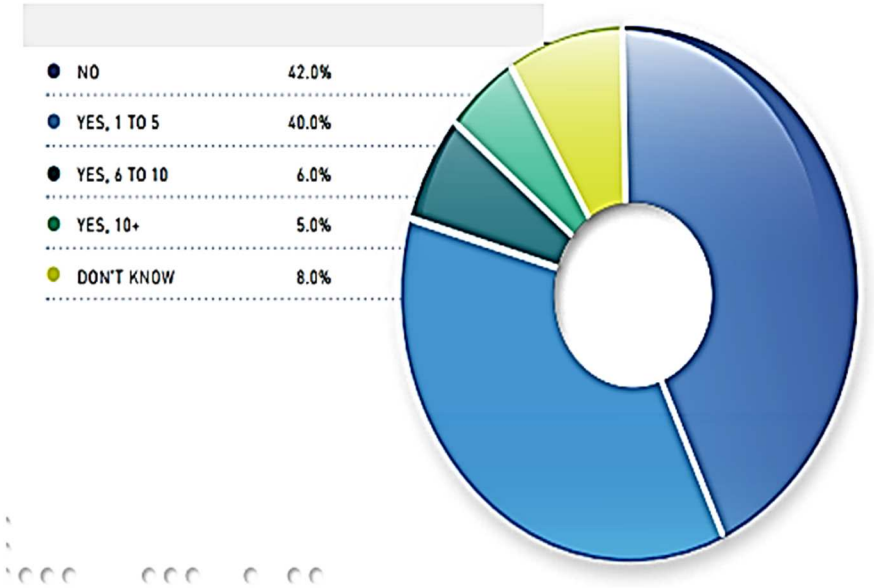
[39] BID, Banco Interamericano de Desarrollo. Informe de Ciberseguridad. [Online]. Observatorio de la ciberseguridad en América Latina y el caribe: 2016. [citado 2016-11-20]. Disponible en internet <http://observatoriociberseguridad.com/graph/countries//selected//0/dimensions/1-2-3-4-5>.

[40] EL NACIONAL, República Dominicana. Líderes de telecomunicaciones plantean a expertos extranjeros situación de ciberseguridad en RD. [Online]. República Dominicana: 2016. [citado 2016-11-20]. Disponible en internet <http://elnacional.com.do/lideres-de-telecomunicaciones-plantean-a-expertos-extranjeros-situacion-de-ciberseguridad-en-rd/>.

[41] AUSTRALIAN, Government. Institute of Criminology. Cybercrime, Cybercrime in focus. [Online]. Australia: 2015. [citado 2016-11-20]. Disponible en internet <http://www.aic.gov.au/crime_types/in_focus/cybercrime.html>.

[42] AUSTRALIAN, Government. Informe 2015 Cyber Security Survey. Major Australian Businesses. Australian Cyber Security Centre: 2015. Pág. 24

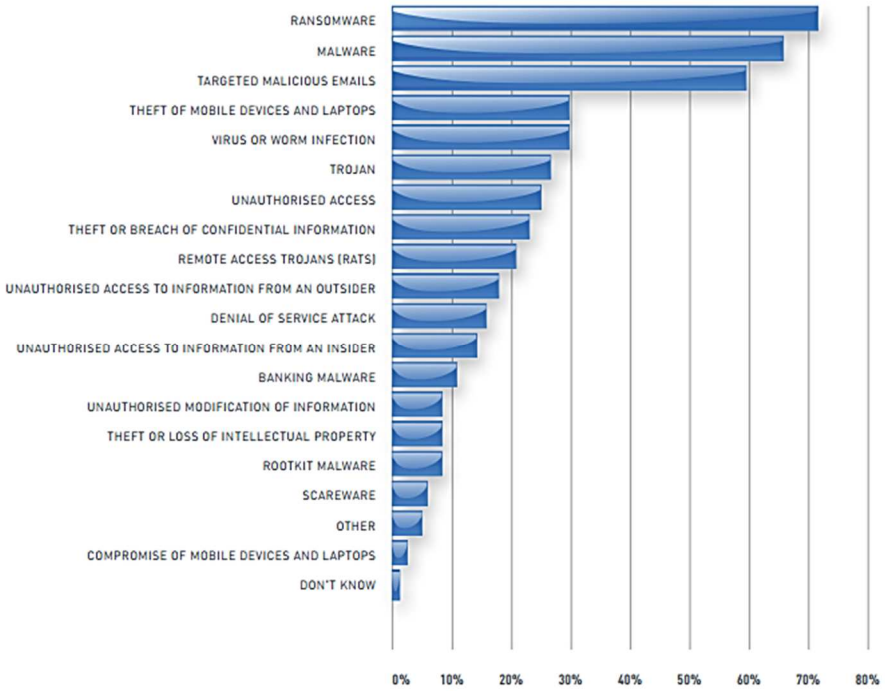
Grafica 5 Número de incidentes de ciberseguridad



Fuente 11 CERT Australia y ASCS Australia. (2015)

Australia es uno de los países más conectados a internet y con una economía muy fuerte, pero esto también ocasiona que sea un atractivo paraíso para los delincuentes informáticos, que ven en estas condiciones una muy valiosa fuente de posibilidades; en la gráfica número 6, se puede observar claramente cuáles son los tipos de ataques que están afectando al país: el ramsomware con un porcentaje mayor al 70%, el malware superior al 65%, correos maliciosos dirigidos de forma específica superior al 55%, son los tres más usuales. El gobierno australiano esta consiente de la problemática y sigue trabajando en mejorar la seguridad informática, muestra de ello fue la firma del convenio de ciberdelincuencia.

Grafica 6 Tipo de incidentes de ciberseguridad



Fuente 12 Cert Australia y ASCS Australia. (2015).

La legislación está contemplada dentro de:

- ✓ “Ley de la ciberdelincuencia 2001 No. 161, 2001
- ✓ Ley para enmendar la legislación relativa a los delitos informáticos, y para otros fines
- ✓ Ley de Organización Australiana de Inteligencia de Seguridad 1979 3
- ✓ Ley de delitos de 1914 3
- ✓ Ley del Código Penal 1995 3
- ✓ Servicios de Educación para Estudiantes Extranjeros, de 2000 14
- ✓ Ley de Telecomunicaciones (interceptación) 1997 14
- ✓ Ley de delitos de 1914 15
- ✓ Ley de aduanas de 1901 19”.[43]

[43] AUSTRALIAN, Government. Federal Register of Legislation. Cybercrime Act 2001. [Online]. Australia: se2016. [citado 2016-11-20]. Disponible en internet <https://www.legislation.gov.au/Details/C2004A00937>.

3.1.4 Israel. Ratifico el Tratado Internacional, el 9 de mayo de 2016 entrando en vigor el 1 de septiembre de 2016. En los estados árabes no existe uno solo que posea o haya promulgado leyes especiales de delitos informáticos e internet.[44]

Cuenta con la ley de computadoras de 1995, (se puede consultar en http://www.cybercrimelaw.net/Israel.html)

Sin embargo, la información en cuanto a estadísticas en el país, no es fácil de conseguir.

3.1.5 Japón. Realizo firma del convenio el 23 de noviembre de 2001, lo ratificó el 3 de julio de 2012, entrando en vigor el 1 de noviembre de 2012, por cuanto en el año 2011 el país aún no contaba con una legislación en este terreno, en vista de que el convenio exige criminalizar el acceso no autorizado a sistemas informáticos, el almacenamiento de pornografía infantil o la vulneración de derechos de autor.[45]

Cuenta con la ley 128 de 1999 que reglamenta el acceso no autorizado a computadores y establece penas desde los 3 meses hasta los 7 años de prisión. (Si se desea ampliar la información se puede consultar en http://www.cybercrimelaw.net/Japan.html)

Pero, la información en cuanto a estadísticas en el país no es fácil de conseguir.

3.1.6 Mauricio. Ratifico el Convenio de Budapest el 15 de noviembre de 2013, entrando en vigor el 3 de enero de 2014. En cuanto a legislación informática cuenta con THE COMPUTER MISUSE AND CYBERCRIME ACT 2003 Act 22 of 2003, en la cual reglamenta lo concerniente al acceso no autorizado a datos, acceso con intención de cometer algún delito, interceptación de datos de carácter informáticos, modificación de material informático, dañar o denegar el acceso a sistemas informáticos, divulgación no autorizada de contraseñas y posesión ilegal de dispositivos y datos, dando origen a penas que van desde 1 año hasta 20 años de servicio o servidumbre y multas desde las 50.000 hasta 200.000 rupias, (para ampliar información consultar en http://www.cybercrimelaw.net/Mauritsius.html), no presenta estadísticas sobre delincuencia en la red y se dificulta encontrar información sobre este país.

---

[44] ELHANEM, Elhanem. Espacio libre dentro de los límites de lo posible, Los delitos cibernéticos. cara fea de la TI. [Online]. Israel: 2016. [citado 2016-11-20]. Disponible en internet < https://elhanem.wordpress.com/للتكنولو-القبيح-الوجه-الانترنت-جرائم>.

[45] NAVEGANTE TECNOLOGIA, El mundo.es Japón aprueba una ley que criminaliza la creación de virus informáticos. [Online]. España: 2011. [citado 2016-11-20]. Disponible en internet <http://www.elmundo.es/elmundo/2011/06/17/navegante/1308304867.html>.

3.1.7 Panamá. Ratifico el Acuerdo el 5 de marzo de 2014 entrando en vigor el 7 de enero de 2014, su aprobación se realizó por el documento aprobado mediante Ley No. 79 de 22 de octubre de 2013, Gaceta Oficial No. 27403-A de 25 de octubre de 2013

Del año 2007 a abril de 2015 el país registró 359 investigaciones con ciberdelitos y solo 3 condenas, desde robo de información hasta hackeo de cuentas de ministerios y funcionarios de alto perfil. 42 de cada 100 personas tienen acceso a internet.[46]

La legislación en cuanto a informática en panamá se encuentra estipulada de la siguiente forma:

- "Derecho Sustantivo
- Delitos informáticos
- Código Penal
- Disposiciones Específicas
- Acceso ilícito: Artículo 283 del Código Penal
- Interceptación ilícita: Artículo 284 del Código Penal
- Interferencia en el Sistema: Artículo 284 del Código Penal
- Falsificación Informática:
- Artículos 362 y 364 del Código Penal
- Artículo 61, Ley 51 de 2008. Documentos y Firmas Electrónica
- Fraude Informático: Artículos 216 y 222 del Código Penal
- Pornografía Infantil: Artículos 181 y 182 del Código Penal
- Derecho Procesal
- Procedimientos para la investigación de Delitos Informáticos
- Código Judicial
- Disposiciones Específicas
- Registro y Confiscación de datos informáticos almacenados: Artículo 2178 Código Judicial
- Obtención en tiempo real de datos sobre el tráfico: Artículo 16 – Ley 16/2004
- Interceptación de Datos sobre el Contenido: Artículo 16 – Ley 16/2004".[47]

Leandro Espinoza, experto en seguridad informática de la UTP (Universidad Tecnológica de Panamá), señala que "No existe personal capacitado para atender los requerimientos en materia de seguridad informática, aún no se ha aprobado la

[46] LA PRENSA, Política. Acechan delitos informáticos. [Online]. Panamá: 2015. [citado 2016-11-20]. Disponible en internet <http://www.prensa.com/politica/Acechan-delitos-informaticos-Panama_0_4220578020.html>

[47] PANAMA, Departamento de cooperación Jurídica. Derecho Sustantivo. [Online]. Panamá: 2016. [citado 2016-11-20]. Disponible en internet <http://www.oas.org/juridico/spanish/cyb_pan.htm>.

ley 105, no hay presupuesto para investigación en ciberseguridad, en la ley no se contempla la usurpación de identidad en redes sociales".[48]

3.1.8 Sudáfrica. Firmo el Convenio el 23 de noviembre de 2001, no ratifico y no ha entrado en vigor, pese a que cuenta con una ley contenida en THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT of July 31 2002, (Act No. 25, 2002) donde se establece legislación para el acceso no autorizado, interceptación e interferencia de datos con penas que van desde uno (1) a cinco (5) años y multas acorde al delito, (si se desea ampliar información se puede consultar en http://www.cybercrimelaw.net/South-Africa.html)

Es muy poco lo que se conoce en datos estadísticos sobre ciberdelincuencia en este país.

3.1.9 Sri Lanka. Ratifico el tratado el 29 de mayo de 2014, entrando en vigor el 9 de enero de 2015, al día de hoy su ley de ciberdelincuencia se encuentra en proceso de aprobación. Prácticamente no existe información sobre delitos informáticos en este país.

3.1.10 Estados Unidos de Norteamérica. Realizó firma del Convenio el 23 de noviembre de 2001, lo ratificó el 29 de septiembre de 2006 entrando en vigor el 1 de enero de 2007, aunque Estados Unidos cuenta con leyes sobre la materia brinda un trato distinto en los diferentes estados, por ejemplo, no hay una ley federal, pero si se reconoce el ciberbullyng en la mayoría de estados.[49]

Es importante recalcar que las técnicas de investigación de Estados Unidos en el ámbito del cibercrimen son de las más avanzadas del mundo, han producido múltiples programas e iniciativas en la lucha contra la trata de seres humanos en su dimensión en la Red.[50]

La legislación referente a delitos informáticos se encuentra contenida en:

UNITED STATES CODE

---

[48] MORALES, Thalia S. Acechan los delitos informáticos en Panamá. [Online]. Panamá: 2015. [citado 2016-11-20]. Disponible en internet <http://www.prensa.com/politica/Acechan-delitos-informaticos-Panama_0_4220578020.html>.

[49] ESPAÑA, Gobierno de. Informe Análisis de derecho comparado sobre ciberdelincuencia, ciberterrorismo y ciberamenzas al menor. España: 2015. Pág. 581

[50] ESPAÑA. Op. Cit. Pág. 581

TITLE 18. CRIMES AND CRIMINAL PROCEDURE

PART I -CRIMES

CHAPTER 47-FRAUD AND FALSE STATEMENTS

Section 1030. Fraud and related activity in connection with computers. (Se puede encontrar en http://www.cybercrimelaw.net/US.html).

3.2 ESTADO ACTUAL

A nivel mundial la empresa de seguridad Gemalto estimó que, tan solo en el primer semestre de 2015, hubo 888 filtraciones, 246 millones de registros afectados. Por su parte, una investigación de IBM, indicó que el costo total consolidado de una brecha de datos promedio en 2014 alcanzó los USD 3,8 millones, lo que marcó un incremento del 23% con respecto a 2013.[51]

El año 2015 en cifras es muy preocupante, según el boletín de seguridad de Kaspersky (compañía internacional dedicada a la seguridad informática).

- ✓ 1,966,324 notificaciones registradas sobre intentos de infecciones de malware con el objetivo robar dinero a través de acceso en línea a cuentas bancarias.
- ✓ Ramsomware detectado en 753.684 computadoras de usuarios únicos
- ✓ El antivirus web de Kaspersky Lab detectó 121.262.075 objetos maliciosos únicos.
- ✓ Las soluciones de Kaspersky Lab repelieron 798.113.087 ataques lanzados desde recursos en línea ubicados en todo el mundo.
- ✓ El 34,2% de las computadoras sufrieron al menos un ataque web durante el año.
- ✓ El 24% de los ataques web neutralizados por los productos de Kaspersky La se realizó utilizando recursos web maliciosos ubicados en los Estados Unidos.
- ✓ Kaspersky Lab. detectaron un total de 4.000.000 de objetos maliciosos y potencialmente no deseado.[52]

Por su parte Symantec (Compañía Americana de Software) en su informe de seguridad del año 2015, refleja un panorama también complejo, en lo concerniente a los ataques sufridos por las empresas, que en un principio eran solo las grandes, pero hoy en día también se ataca a la pequeña y mediana empresa, como se puede

[51] PAGNOTTA, Sabrina. Welivesecurity Noticias, opiniones y análisis de la comunidad de seguridad de ESET, Top 5 de las brechas de datos más devastadoras de 2015. [Online]. Latinoamérica: 2016. [citado 2016-11-20]. Disponible en internet <http://www.welivesecurity.com/la-es/2016/01/08/top-5-brechas-de-datos-devastadoras-2015/>.

[52] KASPERSKY, Security. Moscú: 2015. Pág. 85

ver en la gráfica número siete (7), el sector de servicios sufrió un porcentaje de violaciones por número de incidentes superior al 65% con 200 casos y violaciones por número de identidades expuestas superior al 60% con 259.893.565 incidentes, lo cual es una cifra muy alta con relación a los otros sectores, entre los cuales el que más se le acerco es el de finanzas, con 10.8% de violaciones por número de incidentes y 28.08% en violaciones por número de identidades expuestas.

Grafica 7 Violaciones por número de incidente e identidades expuestas

10 Principales Sectores que Sufrieron Violaciones por Número de Incidentes

- *Los Servicios de Salud son clasificados como un sub-sector dentro del sector de servicios, y 120 de las 200 violaciones que ocurrieron en el sector de servicio fueron atribuidas al segmento de la salud.*

	Sector	Número de Incidentes	% de Incidentes
1	Servicios	200	65,6%
2	Finanzas, Seguros y Mercado Inmobiliario	33	10,8%
3	Comercio Minorista	30	9,8%
4	Administración Pública	17	5,6%
5	Comercio Mayorista	11	3,6%
6	Manufactura	7	2,3%
7	Transporte & Servicios Públicos	6	2,0%
8	Construcción	1	<1%

10 Principales Sectores que Sufrieron Violaciones por Número de Identidades Expuestas

- *El sector de Servicios fue responsable del 60% de las identidades expuestas, la mayoría de las cuales estaban en el sub-sector de Servicios Sociales.*

	Sector	Número de Incidentes	% de Incidentes
1	Servicios	259.893.565	60,6%
2	Finanzas, Seguros y Mercado Inmobiliario	120.124.214	28,0%
3	Administración Pública	27.857.169	6,5%
4	Comercio Mayorista	11.787.795	2,7%
5	Comercio Minorista	5.823.654	1,4%
6	Manufactura	3.169.627	<1%
7	Transporte & Servicios Públicos	156.959	<1%
8	Construcción	3.700	<1%

Fuente 13 https://www.symantec.com/content/dam/symantec/es/docs/reports/istr-21-2016-es.pdf?aid=elq_&om_sem_kw=elq_16612400&om_ext_cid=biz_email_elq_

Es claro que la mayoría de estas violaciones no se originaron por exposiciones a propósito por parte de los empleados, en su mayoría, es evidenciable que muchos casos ocurrieron por diversos factores que permitieron errores que llevaron al incidente, entre los cuales podemos contar con la falta de una adecuada política de seguridad, sistemas débiles, programas con bajos niveles de seguridad, falta de configuración adecuada de los sitios, entre muchos otros.

En la gráfica número 8 se evidencia los Sub-Sectores que sufrieron violaciones por número de incidentes, entre los cuales el que posee el mayor porcentaje es el de servicios de salud con 120 incidentes y un 39.3% muy lejos del siguiente que solo alcanzo un 6.6%; por otra parte, los Sub-Sectores que sufrieron violaciones por número de identidades expuestas, está el de servicios sociales con 191.035.533 y un 44.5% seguido del subsector Aseguradoras con un 23.4%.

Cuando de identidades expuestas, se refiere a información como nombres, direcciones, fechas de nacimiento, números de documento, registros médicos, y cualquier información que en el mercado negro puede tener un uso bastante privilegiado.

Grafica 8 Subsectores que sufrieron violaciones por incidentes e identidades expuestas

10 Principales Sub-Sectores que Sufrieron Violaciones por Número de Incidentes

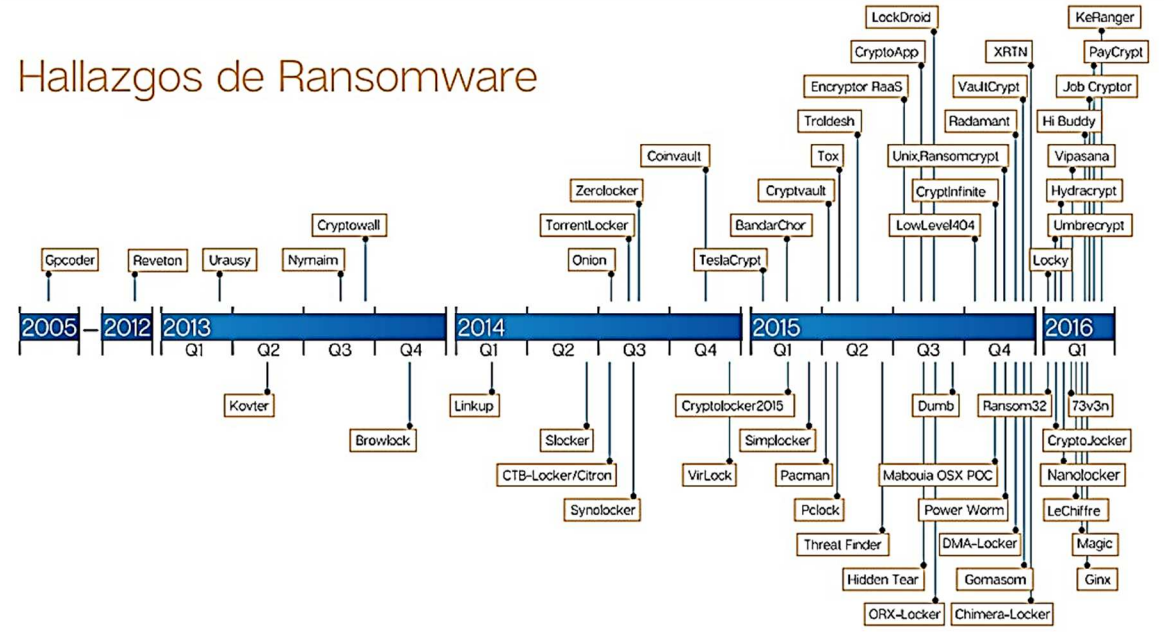
	Sector	Número de Incidentes	% de Incidentes
1	Servicios de Salud	120	39,3%
2	Servicios Empresariales	20	6,6%
3	Servicios Educativos	20	6,6%
4	Aseguradoras	17	5,6%
5	Hoteles y Otros Alojamientos	14	4,6%
6	Comercio Mayorista - Bienes Duraderos	10	3,3%
7	Restaurantes y Bares	9	3,0%
8	Ejecutivo, Legislativo y General	9	3,0%
9	Instituciones Depositarias	8	2,6%
10	Servicios Sociales	6	2,0%

10 Principales Sub-Sectores que Sufrieron Violaciones por Número de Identidades Expuestas

	Sector	Número de Incidentes	% de Incidentes
1	Servicios Sociales	191.035.533	44,5%
2	Aseguradoras	100.436.696	23,4%
3	Servicios Personales	40.500.000	9,4%
4	Administración de Recursos Humanos	21.501.622	5,0%
5	Agentes de Seguros, Correctores y Servicios	19.600.00	4,6%
6	Servicios Empresariales	18.519.941	4,3%
7	Comercio Mayorista - Bienes Duraderos	11.787.795	2,7%
8	Ejecutivo, Legislativo y General	6.017.518	1,4%
9	Servicios Educativos	5.012.300	1,2%
10	Servicios de Salud	4.154.226	1,0%

Fuente 14 https://www.symantec.com/content/dam/symantec/es/docs/reports/istr-21-2016-es.pdf?aid=elq_&om_sem_kw=elq_16612400&om_ext_cid=biz_email_elq_

Figura 4 Línea de tiempo Ransomware

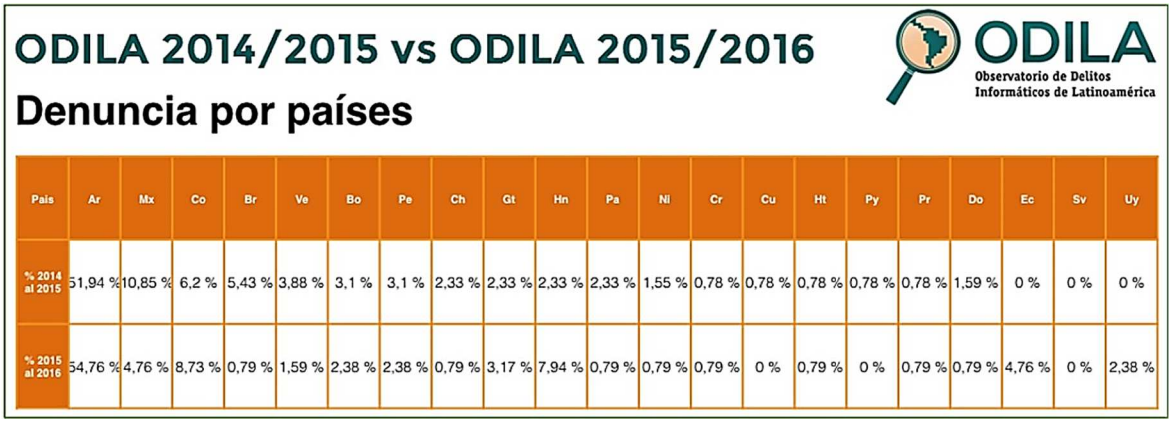


Fuente 15 https://www.symantec.com/content/dam/symantec/es/docs/reports/istr-21-2016-es.pdf?aid=elq_&om_sem_kw=elq_16612400&om_ext_cid=biz_email_elq_

El ramsomware es otra de las formas de ataque que ha evolucionado convirtiéndose en una muy buena fuente de ingresos para los delincuentes, es de aclarar que cualquier persona puede ser víctima de él, y para los gobiernos y autoridades es muy difícil prevenirlo, muestra de ello refleja la figura 4, a través de la cual se aprecia la línea de tiempo en la cual es evidente una evolución bastante agresiva, en el año 2005 solo apareció el Gpcoder y el año 2016 ya existían 15 diferentes tipos entre los cuales están KeRanger, PayCrypt, Job Cryptor, Hi Buddy, Vipasana, Hydracrypt, Umbrecrypt, Locky, Ransom32, 73v3n, Crypto Jocker, Nanolocker, Lechiffre, Magyc y Ginx.

El estado actual en la región de Latinoamérica es un poco abrumador, en reportes como el que presenta ODILA (Observatorio de Delitos Informáticos de Latinoamérica), portal que busca dar a conocer los delitos informáticos y ayudar a la sociedad sobre la legislación vigente, invitando a que la gente realice denuncias formales ante los organismos competentes.

Tabla 4 Denuncia por países



ODILA 2014/2015 vs ODILA 2015/2016

Denuncia por países

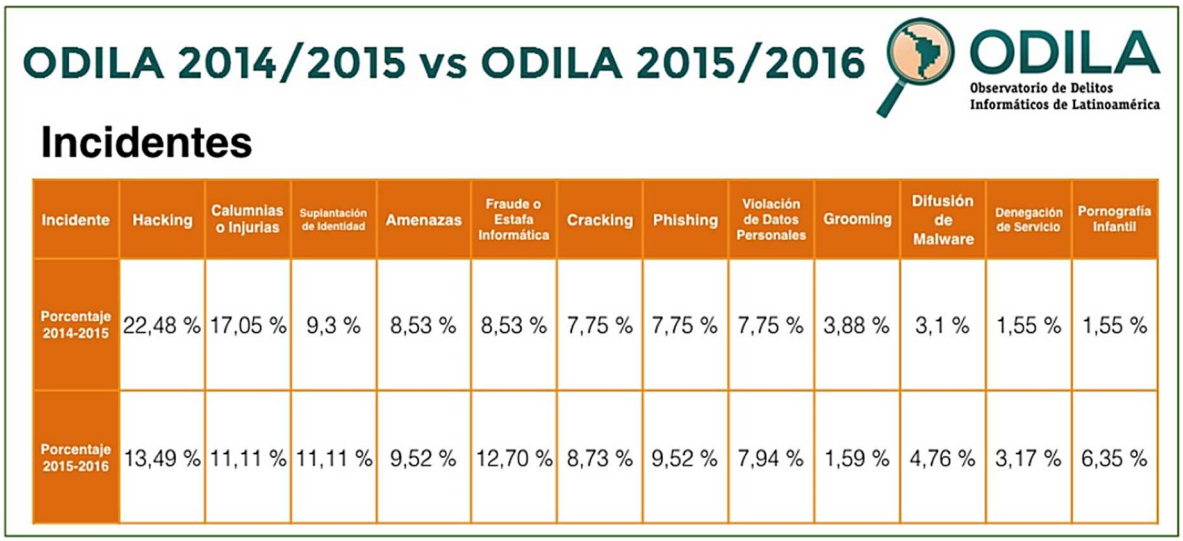
ODILA Observatorio de Delitos Informáticos de Latinoamérica

País	Ar	Mx	Co	Br	Ve	Bo	Pe	Ch	Gt	Hn	Pa	Ni	Cr	Cu	Ht	Py	Pr	Do	Ec	Sv	Uy
% 2014 al 2015	51,94 %	10,85 %	6,2 %	5,43 %	3,88 %	3,1 %	3,1 %	2,33 %	2,33 %	2,33 %	2,33 %	1,55 %	0,78 %	0,78 %	0,78 %	0,78 %	0,78 %	1,59 %	0 %	0 %	0 %
% 2015 al 2016	54,76 %	4,76 %	8,73 %	0,79 %	1,59 %	2,38 %	2,38 %	0,79 %	3,17 %	7,94 %	0,79 %	0,79 %	0,79 %	0 %	0,79 %	0 %	0,79 %	0,79 %	4,76 %	0 %	2,38 %

Fuente 16 https://www.odila.org/pdf/Informe_ODILA_2016.pdf

En la anterior tabla, se puede observar como la mayoría de los países ni siquiera realizan denuncias de los incidentes sucedidos, siendo Argentina el país que más denuncia con un 51.94% seguido de lejos por México con un 10.85% y Colombia con el 6.2% entre el año 2014 y 2015; sin embargo, al ver entre el 2015 y 2016 el nivel de denuncias disminuye en Argentina y México y aumenta en Colombia.

Tabla 5 Incidentes



ODILA 2014/2015 vs ODILA 2015/2016

Incidentes

ODILA Observatorio de Delitos Informáticos de Latinoamérica

Incidente	Hacking	Calumnias o Injurias	Suplantación de Identidad	Amenazas	Fraude o Estafa Informática	Cracking	Phishing	Violación de Datos Personales	Grooming	Difusión de Malware	Denegación de Servicio	Pornografía Infantil
Porcentaje 2014-2015	22,48 %	17,05 %	9,3 %	8,53 %	8,53 %	7,75 %	7,75 %	7,75 %	3,88 %	3,1 %	1,55 %	1,55 %
Porcentaje 2015-2016	13,49 %	11,11 %	11,11 %	9,52 %	12,70 %	8,73 %	9,52 %	7,94 %	1,59 %	4,76 %	3,17 %	6,35 %

Fuente 17 https://www.odila.org/pdf/Informe_ODILA_2016.pdf

La variación en los incidentes es realmente muy poca como se puede ver en la tabla 5, incluso en algunos, aumento drásticamente como en el caso de la pornografía infantil que paso del 1.55% al 6.35%, el más presentado es el hacking con 22.48% entre el 2014 y 2015 que presento disminución hasta el 13.49% entre el 2015 y 2016.

Tabla 6 Causas de no denuncia

¿Ha Denunciado?	No, no denuncié porque...	Si, ya denuncie y la investigación está en curso	Si, denuncie pero la investigación no avanzó	Sí, denuncié y ya se ha condenado al o los culpables.
Porcentaje 2014-2015	68,22 %	16,28 %	15,5 %	0 %
Porcentaje 2015-2016	82,54 %	5,56 %	11,11 %	0,79 %

Fuente 18 https://www.odila.org/pdf/Informe_ODILA_2016.pdf

El porcentaje de personas que no denuncian es desesperanzador, como se puede ver en la tabla 6 más del 50%, 68.22% entre 2014 y 2015, 82.54% entre 2015 y 2016; pero el de personas condenadas si es devastador, pues en el último año solo el 0.79% de los denunciados recibieron algún tipo de condena.

Tabla 7 Porque no se denuncia

Causas	No creo que la investigación tenga éxito	No quiero difundir públicamente el incidente (pérdida de	No creo en la Policía ni en la Justicia Penal	No creo que la denuncia sea útil, porque el sistema penal no es apto	Tengo temor de futuras represalias de parte del autor	No sé donde denunciar	No me tomaron la denuncia	En parte me siento culpable por el incidente	No me considero víctima de un delito	Otros
Porcentaje 2014-2015	17,00 %	17,00 %	12,00 %	12,00 %	10,00 %	9,00 %	7,00 %	7,00 %	5,00 %	4,00 %
Porcentaje 2015-2016	16,19 %	12,38 %	8,57 %	5,71 %	16,19 %	19,05 %	4,76 %	0,95 %	13,33 %	2,86 %

Fuente 19 https://www.odila.org/pdf/Informe_ODILA_2016.pdf

En la tabla llama la atención que la mayoría de las personas no denuncia porque no sabe dónde hacerlo (19.05%) y porque no creen que la investigación tenga éxito (19.16%) al igual que el miedo a nuevas represalias (16.19%).

El informe concluye diciendo que con el paso de los años la problemática de los delitos informáticos aumenta y a pesar de crear leyes no son suficientes, falta una legislación procesal más adecuada. Existe falta de estadísticas oficiales (reales y presentadas por cada país) y especificas por delitos y sus objetivos al igual que el daño causado.[53]

3.3 ANÁLISIS DEL CONVENIO DE CIBERDELINCUENCIA DE BUDAPEST

Para comprender la importancia del convenio de Budapest es necesario ver las dimensiones que tiene; el 5 de mayo de 1949 tras la firma de la Carta fundacional -el Tratado de Londres- por parte de Bélgica, Francia, Luxemburgo, Países Bajos y Reino Unido y después, Irlanda, Italia, Dinamarca, Noruega y Suecia nace el consejo de Europa convirtiéndose en la organización internacional más antigua que se encarga de luchar por la Protección de los Derechos Humanos y de las Libertades Fundamentales.[54], posteriormente firmaron como miembros Grecia y Turquía el 9-8-1949, Islandia el 7-3-1950, Austria el 16-4-1956, Chipre el 24-5-1961, Suiza el 6-5-1963, Malta el 29-04-1965, Portugal el 22-09-1976, España el 24-11-1977, Liechtenstein el 23-11-1978, San Marino el 16-11-1988, Finlandia el 5-5-1989, Hungría el 6-11-1990, Polonia el 26-11-1991, Bulgaria el 7-5-1992, Estonia, Lituania y Eslovenia el 14-5-1993, República Checa y Eslovaquia el 30-6-1993, Rumania el 7-10-1993 Andorra el 10-11-1994, Letonia el 10-2-1995, Albania y Moldavia el 13-7-1995, Macedonia el 9-11-1995, Ucrania el 9-11-1995, Rusia el 28-2-1996, Croacia el 6-11-1996, Georgia el 27-4-1999, Armenia y Azerbaiyán el 25-1-2001, Bosnia-Herzegovina el 24-4-2002, Serbia el 3-4-2003, Mónaco el 5-10-2004, Montenegro el 11-05-2007, teniendo al día de hoy 47 miembros.

Es así como el consejo de Europa después de años de estudiar el tema y muchas reuniones, en la 109 decide aprobar el Convenio de ciberdelincuencia de Budapest, al reconocer la necesidad de proteger los intereses legítimos en la utilización y el desarrollo de las tecnologías de la información, y teniendo presente el prevenir los actos que colocan en peligro la confidencialidad, integridad y disponibilidad de los sistemas, redes y datos informáticos de los habitantes.[55]

---

[53] MACEDO, Maximiliano; TEMPERINI, Marcelo y BORGHELLO, Cristian. Reporte ODILA (Observatorio de Delitos Informáticos de Latinoamérica) 2016. Pág. 20

[54] ESPAÑA, Ministerio de asuntos exteriores y cooperación. Consejo de Europa, Historia y actividad del Consejo de Europa. [Online]. España: 2016. [citado 2016-11-20]. Disponible en internet <http://www.exteriores.gob.es/portal/es/politicaexteriorcooperacion/consejodeeuropa/paginas/historiaactividadconsejoeuropa.aspx>.

[55] CONSEJO DE EUROPA, Serie de tratados europeos. Convenio sobre la Ciberdelincuencia. [Online]. Budapest: 2001. [citado 2016-11-20]. Disponible en internet <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41c>.

El convenio cuenta con 26 hojas y está dividido en cuatro capítulos los cuales a su vez se subdividen en secciones y artículos. A continuación, se dará una mirada leve a la construcción del documento.

Capítulo 1. Terminología consta del articulo 1 definiciones, en el cual se exponen “sistema informático”, “datos informáticos”, “proveedor de servicios”, y “datos relativos al tráfico”

Capítulo 2. Medidas que se deben adoptar a nivel nacional, consta de 3 secciones entre las cuales se tienen:

Sección 1 Derecho penal sustantivo en la cual se hace hincapié en que cada parte (país miembro o adherido) deberá adoptar medidas legislativas y de otro tipo necesarias para tipificar los delitos que contiene los artículos del 2 al 13 donde se tratan los temas:

- Acceso ilícito
- Interceptación ilícita
- Ataques a la integridad de datos (acto deliberado, dañe, borre, deteriore, altere o suprima datos informáticos)
- Ataques a la integridad del sistema (por medio de introducción, transmisión, daño, borrado, deterioro, alteración o supresión)
- Abuso de dispositivos (producción, venta, utilización, importación, difusión u otras, incluidos artículos 1 al 5)
- Falsificación informática (introducción, alteración, borrado o supresión de datos informáticos)
- Fraude informático (introducción, alteración, borrado o supresión de datos informáticos y cualquier interferencia en el funcionamiento de un sistema informático)
- Delitos relacionados con la pornografía infantil (Producción, oferta, difusión, adquisición y posesión a través de sistemas informáticos. Menores de 18 años, en algunos casos se puede exigir para menores de 16 por solicitud de la parte)
- Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines (aplicación de la Convención Internacional sobre la Protección de los Artistas Intérpretes o Ejecutantes, “Convención de Roma”)
- Tentativa de complicidad (aplica artículos del 2 al 10)
- Responsabilidad de personas jurídicas (podrá ser penal, civil o administrativa; sin perjuicio de la responsabilidad penal de las personas físicas)

- Sanciones y medidas. (cada parte garantizara la imposición de las sanciones).[56]

Sección 2 Derecho procesal en la cual se hace hincapié en que cada parte (país miembro o adherido) deberá adoptar medidas legislativas y de otro tipo necesarias para establecer los poderes y procedimientos previstos para efectos de investigación penal consta de los artículos del 14 al 21 donde se tratan los temas

- Ámbito de aplicación de las disposiciones de procedimiento
- Condiciones y salvaguardias (cada parte debe garantizar una protección adecuada de los derechos humanos y de las libertades fundamentales)
- Conservación rápida de datos informáticos almacenados
- Conservación y revelación parcial rápidas de los datos relativos al trafico
- Orden de presentación
- Registro y confiscación de los datos informáticos almacenados
- Obtención en tiempo real de datos relativos al trafico
- Interceptación de datos relativos al contenido (obtener o grabar con medios técnicos y obligar a un proveedor de servicios a realizarlo y además prestar apoyo y asistencia).[57]

Sección 3 Jurisdicción en esta sección trata de que cada parte debe adoptar las medidas legislativas y de otro tipo necesarias para afirmar su jurisdicción cuando se trata de los artículos 2 al 11 y siempre y cuando el delito se haya cometido en su territorio ya sea por vía terrestre o aérea. Se encuentra en el artículo 22.

Capítulo 3. Cooperación internacional, este consta de dos secciones las cuales son:

Sección 1 Principios generales que comprende los artículos del 23 al 28 y trata temas como son:

- Principios generales relativos a la cooperación internacional
- Extradición (artículos del 2 al 11, sujeto a condiciones previstas en el derecho interno de la parte requerida)
- Principios generales relativos a la asistencia mutua
- Información espontanea
- Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables

---

[56] CONSEJO DE EUROPA, Serie de tratados europeos. Op. Cit. Disponible en internet <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41c>.

[57] CONSEJO DE EUROPA, Serie de tratados europeos. Op. Cit. Disponible en internet <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41c>.

- Confidencialidad y restricciones de uso.[58]

Sección 2 Disposiciones específicas del articulo 29 al 35 donde se tratan temas de asistencia mutua como son:

- Conservación rápida de datos informáticos almacenados
- Revelación rápida de datos conservados (podrá ser negada cuando la parte requerida lo considera de carácter político o atenta contra la soberanía, seguridad, orden público u otro esencial)
- Asistencia mutua en relación con los poderes de investigación
- Acceso transfronterizo a datos almacenados, con consentimiento o cuando sean accesibles al publico
- Asistencia mutua para la obtención en tiempo real de datos relativos al trafico
- Asistencia mutua en relación con la interceptación de datos relativos al contenido
- Red 24/7 (Cada parte garantiza asistencia inmediata en asesoramiento técnico, conservación de datos, suministro de información de carácter jurídico y localización de sospechosos).[59]

Capítulo 4. Clausulas finales con los artículos del 36 al 48 y contiene temas de alta relevancia como son:

- Firma y entrada en vigor (el convenio está sujeto a ratificación, aceptación y aprobación)
- Adhesión al convenio (por medio de invitación)
- Aplicación territorial (cada parte decide el territorio sobre el cual se aplicará el convenio)
- Efectos del convenio
- Declaraciones
- Clausula federal
- Reservas (se pueden realizar sobre: párrafo 2 artículo 4, párrafo3 artículo 6, párrafo 4 artículo 9, párrafo 3 artículo 10, párrafo 3 artículo 11, párrafo 3 artículo 14, párrafo 2 artículo 22, párrafo 4 artículo 29, párrafo 1 artículo 41 y solo al momento de la firma mediante escrito)
- Mantenimiento y retirada de las reservas
- Enmiendas
- Solución de controversias
- Consulta entre partes

---

[58] CONSEJO DE EUROPA, Serie de tratados europeos. Op. Cit. Disponible en internet <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41c>.

[59] CONSEJO DE EUROPA, Serie de tratados europeos. Op. Cit. Disponible en internet <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41c>.

- Denuncia
- Notificación.[60]

3.4 REQUERIMIENTOS PARA UNA ADHESIÓN

El proceso general es el mismo que para adhesión a cualquier convenio y se resume en:

- En principio, el Comité de Ministros podrá tomar la iniciativa de invitar a un Estado no miembro a adherirse. El Estado no miembro solicita la adhesión en una carta dirigida al Secretario General del Consejo de Europa. La carta debe ser firmada por el Ministro de Relaciones Exteriores o un representante que actúe vía diplomática siguiendo instrucciones de su gobierno.
- Las solicitudes formales de adhesión son examinadas por un grupo Relator del Comité de Ministros y, a continuación, por el Comité de Ministros. La decisión de invitar al Estado se toma a nivel de representantes de los ministros. El Comité de Ministros decidió, en abril de 2013, limitar la validez de las invitaciones a un período de cinco años.
- Una invitación para acceder a uno de los convenios del Consejo de Europa se notifica al Estado y antes de que se adhiera, tiene que tomar las medidas necesarias para garantizar que su legislación nacional permite que el convenio se aplique.
- El instrumento de adhesión se depositará en la sede del Consejo de Europa en Estrasburgo, en presencia de un representante del Estado adherente y del Secretario General del Consejo de Europa o de su adjunto. El representante del Estado adherente trae con él o ella el instrumento de adhesión, y un acta del depósito firmado por ambas Partes.
- Las declaraciones o reservas se deben hacer al depositar el instrumento de adhesión.[61]

3.5 SITUACION DE COLOMBIA

Colombia ha presentado avances desde el año 2005 cuando creo la norma de calidad de gestión de la información para las entidades nacionales; en el año 2009 modifico el Código Penal incluyendo la protección de información y datos como bien

---

[60] CONSEJO DE EUROPA, Serie de tratados europeos. Op. Cit. Disponible en internet <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41c>.

[61] COUNCIL OF EUROPE, General information. Participation of Non-member States. [Online]. Estrasburgo: 2016. [citado 2016-11-20]. Disponible en internet <http://www.coe.int/en/web/conventions/participation-of-non-member-states>.

jurídico y el 14 de julio de 2011, con el documento COMPES determinando una estrategia más fuerte orientada a generar unos lineamientos de política para ciberseguridad y ciberdefensa. Envió solicitud para adherirse al convenio de ciberdelincuencia a comienzos del 2012 y ese mismo año en septiembre recibió la invitación para firmar como país adherido.

En materia legal se cuenta con:

- Ley 527 de 1999 - define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación.[62]
- Ley 599 de 2000 - expide el Código Penal Colombiano. Mantuvo la estructura del tipo penal de "violación ilícita de comunicaciones", creó el bien jurídico de los derechos de autor e incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. igualmente tipificó el "Acceso abusivo a un sistema informático".[63]
- Decreto 1524 de 2002 - reglamenta el artículo 5o. de la Ley 679 de 2001 referente a Pornografía en menores de edad.[64]
- Ley 1266 de 2008 - dicta las disposiciones generales del hábeas data y regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.[65]

---

[62] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 527 de 1999. (18, agosto, 1999). por la cual se definen y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación. [en línea]. <http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/LEY_527_DE_1999.pdf> [citado en 7 de octubre 2016]

[63] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 599 de 2000. (24, julio, 2000). por la cual se Expide el Código Penal. En esta se mantuvo la estructura del tipo penal de "violación ilícita de comunicaciones", se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. [en línea]. <http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html> [citado en 7 de noviembre 2016]

[64] COLOMBIA, MINISTERIO DE COMUNICACIONES. Decreto 1524 de 2002. (30, julio, 2002). El cual reglamenta el artículo 5o. de la Ley 679 de 2001 referente a Pornografía en menores de edad. [en línea]. <http://www.icbf.gov.co/cargues/avance/docs/decreto_1524_2002.htm> [citado en 7 de noviembre 2016]

[65] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley Estatutaria 1266. (31, diciembre, 2008). Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países. [en línea]. <https://www.bancoldex.com/documentos/1291_Ley_1266_de_2008_(Habeas_Data).pdf> [citado en 7 de noviembre 2016]

- Ley 1341 de 2009 - define principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la Información y las Comunicaciones –TIC, crea la Agencia Nacional del Espectro.[66]
- Ley 1336 de 2009 - adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes.[67]
- Ley 1273 de 2009 - modifica el Código Penal, crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.[68]
- Ley 1581 de 2012 - dicta disposiciones generales para la protección de datos personales.[69]
- CONPES 3701 - Lineamientos de política para ciberseguridad y ciberdefensa.[70]
- CONPES 3854 - Política nacional de seguridad digital[71]

Colombia ha puesto en marcha iniciativas como Gobierno en Línea, SASIGEL y En TIC Confió, al igual que el centro Cibernético Policial donde se puede ver una

---

[66] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1341 de 2009. (30, julio, 2009). por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones - TIC-, se crea la agencia nacional del espectro y se dictan otras disposiciones. [en línea]. <http://www.mintic.gov.co/portal/604/articles-3707_documento.pdf> [citado en 7 de noviembre 2016]

[67] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1336 de 2009. (21, julio, 2009). por la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes. [en línea]. <http://www.anato.org/sites/default/files/Ley1336de2009.pdf> [citado en 17 de noviembre 2016]

[68] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1273 de 2009. (05, enero, 2009). por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. [en línea]. <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492> [citado en 17 de noviembre 2016]

[69] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1581 de 2012. (17, octubre, 2012). por la cual se dictan disposiciones generales para la protección de datos personales. [en línea]. <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981> [citado en 7 de octubre 2016]

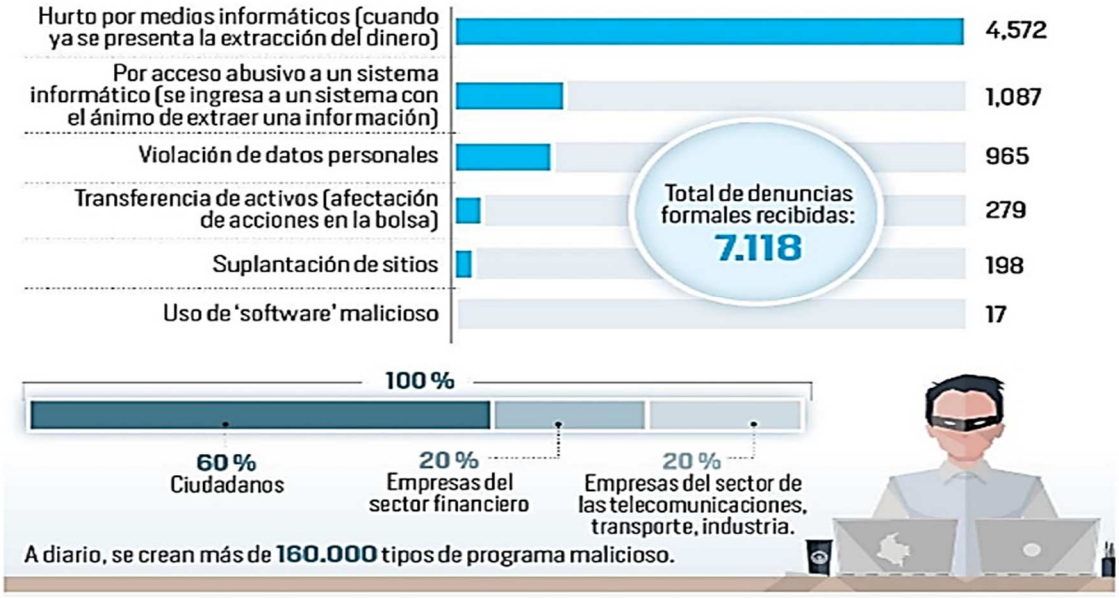
[70] REPUBLICA DE COLOMBIA, Consejo Nacional de Política Económica y Social. CONPES 3701(14, julio, 2011). Lineamientos de política para ciberseguridad y ciberdefensa. [en línea]. <http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf> [citado en 17 de noviembre 2016]

[71] REPUBLICA DE COLOMBIA, Consejo Nacional de Política Económica y Social. CONPES 3854 (11, abril, 2016). Política nacional de seguridad digital. [en línea]. <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf> [citado en 17 de noviembre 2016]

radiografía de los delitos que se comenten en tiempo real e información que puede ayudar al ciudadano, en algunos países de América Latina.

Colombia es tomado como un referente al igual que México, país con el que ha está trabajando de la mano según palabras del Ministro de Tecnologías de la Información y las Comunicaciones (TIC), David Luna[72].

Figura 5 Radiografía de los delitos informáticos en Colombia 2015

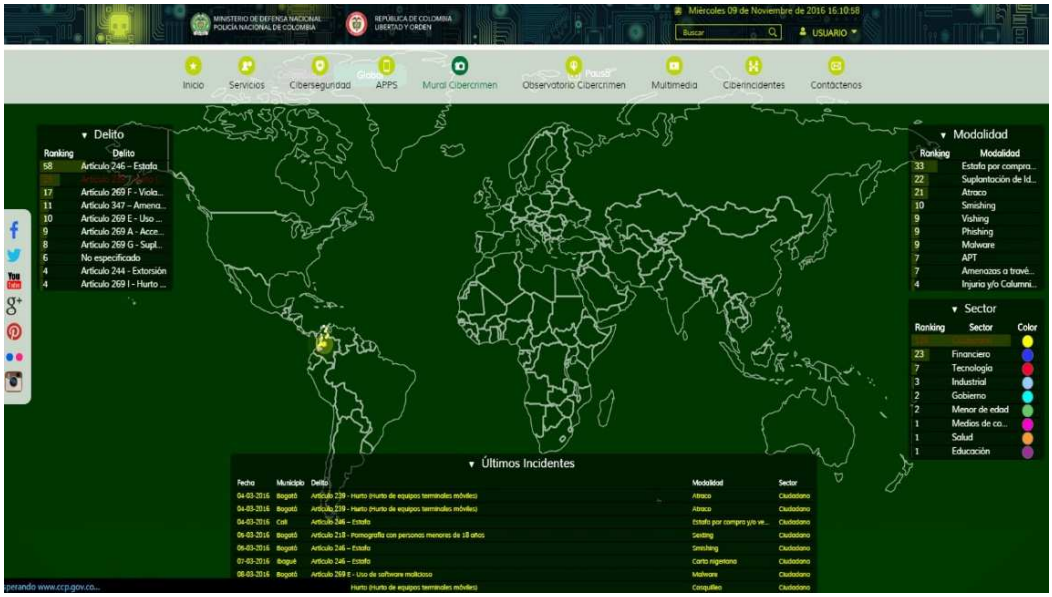


Fuente 20 http://www.eltiempo.com/tecnosfera/tutoriales-tecnologia/cuantos-delitos-informaticos-se-denuncian-en-colombia/16493604

La figura 5 muestra el panorama colombiano durante el 2015, donde el hurto por medios informáticos (4.527 casos) es el que más se presenta, aunque en este solo se cuenta cuando el dinero ya ha sido sustraído, seguido del acceso no autorizado a sistemas con 1.087 casos y violación de datos personales 965 casos, claro que esta es la información denunciada, la cual según indican las autoridades, es muy inferior a la real.

[72] EDITOR, El economista. Colombia es referente mundial en la lucha contra la ciberdelincuencia. [Online]. Colombia 2016- [citado 2016-11-20]. Disponible en internet <http://www.eleconomistaamerica.co/telecomunicacion-tecnologia-co/noticias/7946347/11/16/Colombia-es-referente-mundial-en-la-lucha-contra-la-ciberdelincuencia.html>

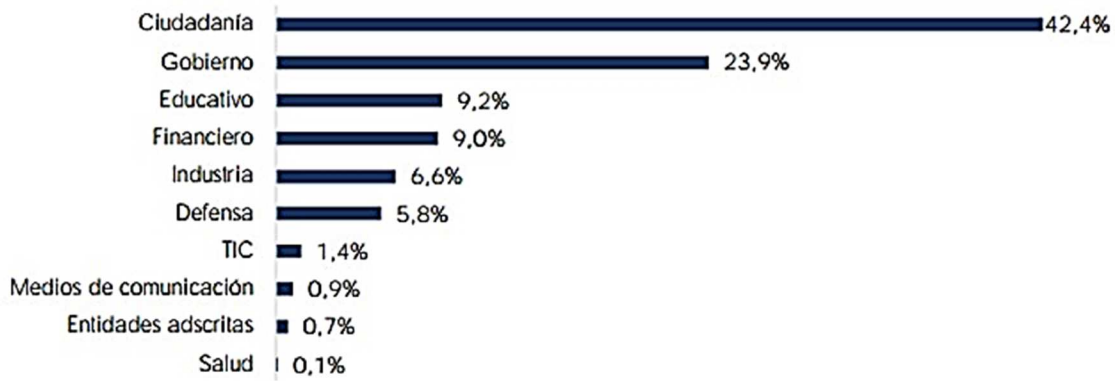
Figura 6 Centro cibernético policial Incidentes en tiempo real



Fuente 21 http://www.ccp.gov.co/ciberincidentes/tiempo-real

La figura 6 nos muestra la información que se presenta en el centro cibernético policial en el cual se pueden consultar los incidentes en tiempo real.

Grafica 9 Sectores afectados en Colombia



Fuente 22 Documento COMPES 3854

La grafica 9 nos muestra claramente que el sector con mayor afectación es la ciudadanía con un 42.4%, posteriormente el gobierno con un 23%, lo cual tal vez obedece a la implementación del sistema GEL y SASIGEL que blinda un poco mejor las plataformas del estado.

En el Documento CONPES 3854 de abril de 2016 el gobierno habla sobre la importancia que tiene el entorno digital en cuanto al desarrollo económico, razón por la cual el Estado debe encontrar la forma de involucrar a todas las partes logrando responder positivamente a cualquier amenaza posible, para esto determino atender los cinco principales problemas:

1. No existe una visión estratégica en seguridad digital basada en la gestión de riesgos
2. Las múltiples partes interesadas no maximizan sus oportunidades al desarrollar actividades socioeconómicas en el entorno digital
3. Se necesita reforzar las capacidades de ciberseguridad con un enfoque de gestión de riesgos de seguridad digital
4. Se necesita reforzar las capacidades de ciberdefensa con un enfoque de gestión de riesgos de seguridad digital
5. Los esfuerzos de cooperación, colaboración y asistencia, nacional e internacional, relacionados con la seguridad digital no son suficientes y requieren ser articulados. [73]

[73] REPUBLICA DE COLOMBIA, Consejo Nacional de Política Económica y Social. CONPES 3854 Op. Cit. Disponible en internet <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf>

4. RESULTADOS

4.1 CUADRO LEGISLACIONES PAISES DENTRO DEL CONVENIO BUDAPEST

El presente cuadro refleja datos relacionados con la legislación que algunos países poseen frente al problema planteado en este documento y unas observaciones sobre el particular.

Tabla 8 Comparativa legislación

Tabla 9 (Continuación)

País	Legislación existente	Legislación faltante	Observaciones
Australia	Centro Australiano de Seguridad Cibernética (ACSC) "Ley de la ciberdelincuencia 2001 No. 161, 2001 Ley para enmendar la legislación relativa a los delitos informáticos, y para otros fines Ley de Organización Australiana de Inteligencia de Seguridad 1979 Ley de delitos de 1914 Ley del Código Penal 1995 Servicios de Educación para Estudiantes Extranjeros, de 2000 Ley de Telecomunicaciones (interceptación) 1997 Ley de delitos de 1914 Ley de aduanas de 1901.[74]	Leyes contra la xenofobia	Tiene una Estrategia de Seguridad Cibernética bien definida, desarrollada en más de 18 meses con consulta de más de 190 organizaciones, negocios, el gobierno y el mundo académico, del país y fuera de él.[75] Costo estimado 491 millones de dólares para los próximos 4 años.[76]
Canadá	La ley en contra del delito informático se encuentra tipificada en el código penal en las secciones 184 (privacidad), 342 (robo, falsificación y uso no autorizado de equipo), 402 (robo de identidad), 403	Leyes contra la xenofobia. Ley que penalice la ingeniería social.	Posee buena legislación, infraestructura, pero su gente no recibe la suficiente capacitación y hay falta de denuncias.

[74] AUSTRALIAN, Federal Register of Legislation. Cybercrime Act 2001. [Online]. Australia: 2016- [citado 2016-11-20]. Disponible en internet <https://www.legislation.gov.au/Details/C2004A00937>.
[75] AUSTRALIAN, Government Atorney-General's Department. www.ag.gov.au, Cyber security. [Online]. Australia: 2016- [citado 2016-11-20]. Disponible en internet <https://www.ag.gov.au/RightsAndProtections/CyberSecurity/Pages/default.aspx>.
[76] EFE, Agencia. Australia anuncia una estrategia de ciberseguridad frente a ataques cibernéticos. [Online]. España: 2016- [citado 2016-11-20]. Disponible en internet <http://www.efe.com/efe/espana/portada/australia-anuncia-una-estrategia-de-ciberseguridad-frente-a-ataques-ciberneticos/10010-2903210>.

Tabla 9 (Continuación)

País	Legislación existente	Legislación faltante	Observaciones
	(fraude de identidad), 490 (delincuentes sexuales de la información).[77]		
Estados Unidos	United States Code Title 18 Crimes and Criminal Procedure, Part 1- Crimes, Chapter 47 Fraud and False Statements, section 1030 Fraud and related activity in connection with computers. Ley federal de Protección de Sistemas Ley federal sobre Fraude mediante transmisiones por cable Electronic communications privacy act Small business computer security and education act Acta federal contra el abuso computacional Economic espionage act Anticounterfeiting consumer protect Criminal copyright infringement statute National stolen property act	Leyes contra la xenofobia. Ley que penalice la ingeniería social.	Posee muy Buena legislación, pero su aplicación suele ser distinta dependiendo del estado, donde ocurra el incidente.
Israel	ley de computadoras de 1995	Leyes contra la xenofobia. Ley que penalice la ingeniería social.	Es uno de los líderes de la seguridad cibernética junto con EEUU, China, Rusia y el Reino Unido, invierte mucho dinero en esta temática. Tiene a favor que su legislación es fuerte.
Japón	Código penal, Ley 128 de acceso no autorizado 1999	Leyes contra la xenofobia. Ley que penalice la ingeniería social.	Ha empezado a trabajar más fuerte en esta materia, se ha dado cuenta que es muy vulnerable, posee buena cantidad de recursos financieros y tecnológicos para hacer frente a la problemática.
Panamá	"Derecho Sustantivo Delitos informáticos Código Penal Disposiciones Específicas Acceso ilícito: Artículo 283 del Código Penal Interceptación ilícita: Artículo 284 del Código Penal	Leyes contra la xenofobia. Ley que penalice la ingeniería social. Fortalecimiento de las penas.	Espera más cooperación internacional, mejorar capacitación y fortalecer penas.

[77] CANADA, Government of. Justice Laws Website. Op. Cit. Disponible en internet <http://laws-lois.justice.gc.ca/eng/acts/c-46/index.html>.

Tabla 9 (Continuación)

País	Legislación existente	Legislación faltante	Observaciones
	Interferencia en el Sistema: Artículo 284 del Código Penal Falsificación Informática: Artículos 362 y 364 del Código Penal Artículo 61, Ley 51 de 2008. Documentos y Firmas Electrónica Fraude Informático: Artículos 216 y 222 del Código Penal Pornografía Infantil: Artículos 181 y 182 del Código Penal Derecho Procesal Procedimientos para la investigación de Delitos Informáticos Código Judicial Disposiciones Específicas Registro y Confiscación de datos informáticos almacenados: Artículo 2178 Código Judicial Obtención en tiempo real de datos sobre el tráfico: Artículo 16 – Ley 16/2004 Interceptación de Datos sobre el Contenido: Artículo 16 – Ley 16/2004".[78]		
República Dominicana	Ley No. 53-07 contra crímenes y delitos de alta tecnología	Leyes contra la xenofobia. Ley que penalice la ingeniería social.	Aún se encuentra en trámite, al igual que la iniciativa del desarrollo de una Estrategia Nacional de Seguridad Cibernética
Mauricio	The Computer Misusse and Cybercrime Act. 2003	Leyes contra la xenofobia. Ley que penalice la ingeniería social.	La información es mínima y los recursos de la isla son muy limitados.
Colombia	Ley 527 de 1999 Acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación.[79]	Leyes contra la xenofobia. Ley que penalice la ingeniería social.	La evolución de Colombia ha sido gradual y está siendo tomado como referente en la región junto a México que ha realizado

[78] PANAMA, Departamento de cooperación Jurídica. Derecho sustantivo. [Online]. Panamá: 2016-[citado 2016-11-20]. Disponible en internet <http://www.oas.org/juridico/spanish/cyb_pan.htm>.
[79] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 527 de 1999. (18, agosto, 1999). por la cual se definen y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación. [en línea]. <http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/LEY_527_DE_1999.pdf> [citado en 7 de octubre 2016]

Tabla 9 (Continuación)

País	Legislación existente	Legislación faltante	Observaciones
	Ley 599 de 200 Expide el Código Penal., se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, "Acceso abusivo a un sistema informático"[80] Decreto 1524 de 2002 Pornografía en menores de edad.[81] Ley 1266 de 2008 Hábeas data y se regula el manejo de la información contenida en bases de datos personales.[82] Ley 1341 de 2009 principios y conceptos sobre la sociedad de la información y la organización de las TIC, se crea la Agencia Nacional del Espectro.[83] Ley 1336 de 2009 robustece la ley 679 de 2001de lucha contra la explotación, la pornografía y el turismo sexual con adolescentes.[84]		grandes adelantos en esta materia. Sin embargo, es prioritario que el país legisle sobre la ingeniería social y la xenofobia, aumente la capacitación en la temática de seguridad informática, y garantice un presupuesto acorde con la problemática actual. Actualmente el país cumple con los requisitos mínimos y una legislación adecuada para pertenecer al convenio de ciberdelincuencia de Budapest, también se ha convertido en un referente a nivel regional junto con México y Brasil.

[80] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 599 de 2000. (24, julio, 2000). por la cual se Expide el Código Penal. En esta se mantuvo la estructura del tipo penal de "violación ilícita de comunicaciones", se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. [en línea]. <http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html> [citado en 7 de noviembre 2016]

[81] COLOMBIA, MINISTERIO DE COMUNICACIONES. Decreto 1524 de 2002. (30, julio, 2002). El cual reglamenta el artículo 5o. de la Ley 679 de 2001 referente a Pornografía en menores de edad. [en línea]. <http://www.icbf.gov.co/cargues/avance/docs/decreto_1524_2002.htm> [citado en 7 de noviembre 2016]

[82] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley Estatutaria 1266. (31, diciembre, 2008). Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países. [en línea]. <https://www.bancoldex.com/documentos/1291_Ley_1266_de_2008_(Habeas_Data).pdf> [citado en 7 de noviembre 2016]

[83] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1341 de 2009. (30, julio, 2009). por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones - TIC-, se crea la agencia nacional del espectro y se dictan otras disposiciones. [en línea]. <http://www.mintic.gov.co/portal/604/articles-3707_documento.pdf> [citado en 7 de noviembre 2016]

[84] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1336 de 2009. (21, julio, 2009). por la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo

Tabla 9 (Continuación)

País	Legislación existente	Legislación faltante	Observaciones
	Ley 1273 de 2009 Modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.[85] Ley 1581 de 2012 protección de datos personales.[86]		

Fuente 23 El autor

4.2 CUMPLIMIENTO DE COLOMBIA PARA ENTRAR AL CONVENIO DE BUDAPEST.

Es importante recordar que el convenio de Budapest es un marco general y guía, mediante la cual los países pueden comenzar a regular su legislación en aras de luchar contra la ciberdelincuencia. En este orden de ideas, Colombia cuenta con los requisitos necesarios para lograr ser aceptado dentro del Convenio.

Actualmente Colombia cuenta con leyes y sanciones para todo lo estipulado en el convenio como es:

- Acceso ilícito
- Interceptación ilícita
- Interferencia en los datos
- Interferencia en el sistema

sexual con niños, niñas y adolescentes. [en línea]. <http://www.anato.org/sites/default/files/Ley1336de2009.pdf> [citado en 17 de noviembre 2016]

[85] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1273 de 2009. (05, enero, 2009). por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. [en línea]. <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492> [citado en 17 de noviembre 2016]

[86] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1581 de 2012. (17, octubre, 2012). por la cual se dictan disposiciones generales para la protección de datos personales. [en línea]. <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981> [citado en 7 de octubre 2016]

- Abuso de los dispositivos
- Falsificación informática
- Fraude informático
- Delitos relacionados con la pornografía infantil
- Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines
- Tentativa y complicidad
- Responsabilidad de las personas jurídicas

También se ha esmerado en la mejora de procesos tales como:

- Conservación rápida de datos informáticos almacenados
- Conservación y revelación parcial rápidas de datos sobre el tráfico
- Registro y confiscación de datos informáticos almacenados
- Obtención en tiempo real de datos sobre el tráfico
- Interceptación de datos sobre el contenido

4.3 VENTAJAS Y DESVENTAJAS DE LA ADHESIÓN

4.3.1 El camino de Colombia hacia la aplicación del Acuerdo Internacional de Budapest

Como se ha visto a través de todo el texto, pertenecer al convenio de ciberdelincuencia de Budapest puede resultar ser muy importante en materia de colaboración internacional, capacitación y lucha contra la delincuencia informática en todas sus formas, sin embargo, se debe tener muy presente los requerimientos al momento de comenzar a formar parte del mismo.

El país requiere realizar mayor inyección de capital en esta temática para destinarlo a la adquisición de equipos, capacitación del sector laboral, judicial y académico, de tal forma que permita comprender los riesgos a que se están expuestos los ciudadanos, las empresas y diferentes organizaciones, así como también judicializar los posibles infractores.

Por su parte, los funcionarios encargados de investigar y juzgar esta clase de delitos, deben prestar toda su voluntad, ante la posibilidad de que haya impunidad, dado que ello seguirá ocasionando que no haya denuncia por parte de las víctimas, como se aprecia en las estadísticas y por consiguiente, se genere un incremento en esta modalidad delincuencial.

En esta dirección, también se requiere que la imposición de penas sea endurecida y el sistema carcelario mejorado de forma integral, para propender por la resocialización del individuo.

Se requiere la unificación del marco jurídico, de tal forma que permita observar, facilitar y acceder a su consulta, cualquier ciudadano, sin temor a conocer sólo una parte del desarrollo que ha adelantado Colombia frente a la ciberdelincuencia.

Los sistemas de denuncias y la información referente a la ciberdelincuencia deben ser más accesibles y fáciles de realizar tanto en operatividad como en estadísticas, diseño y participación de los colombianos.

Se deben crear mecanismos que permitan realizar un adecuado tratamiento de los impactos sufridos por la ciberdelincuencia.

El Estado debe comprometerse con destinar un buen capital para la realización de la estrategia de seguridad informática a nivel nacional.

4.3.2 El camino de Colombia sin la adhesión

Por muchos esfuerzos que se realicen, el no pertenecer a este Convenio limita las posibilidades del país en el evento de solicitar apoyo, colaboración o capacitación, ante la emergencia de bandas criminales organizadas en la modalidad de delitos informáticos, dado que es sabido que, si por ejemplo, ocurre algún delito que tenga impacto en territorio colombiano y el infracto está localizado en otro país miembro del convenio, difícilmente brinda colaboración, ante la ausencia de obligaciones, deberes y derechos de reciprocidad que normalmente contiene los tratados internacionales.

Por otra parte, es innegable el hecho de que Colombia no tiene la capacidad financiera suficiente para estar a la altura de países como Estados Unidos, Reino Unido, China, Israel o Rusia que destinan grandes cantidades de capital a combatir la ciberdelincuencia.

Sin la adhesión al convenio, el país debe invertir más dinero en capacitación de sus diferentes centros de reacción.

Además, es imposible que un país logre luchar de forma unilateral contra la ciberdelincuencia, la colaboración internacional con otros estados y entre la empresa privada y la empresa pública es fundamental para que se pueda combatir el flagelo de la delincuencia informática.

4.4 PROPUESTA

Como es concluyente a través de la investigación realizada, se puede ver que el camino recorrido por Colombia en esta última década, ha tenido por objeto el forjar una senda que permita el establecimiento de una política de ciberseguridad basada en muchos aspectos del convenio de ciberdelincuencia de Budapest, el marco jurídico existente al día de hoy es bueno, aunque presenta algunas falencias que deberán ser corregidas.

Los antecedentes demuestran que el Gobierno debe fortalecerse más para proteger su economía y a sus habitantes ante los diferentes ataques perpetrados por los ciberdelincuentes.

Las dimensiones y alcance del convenio de ciberdelincuencia de Budapest son de orden internacional, permiten a los países adheridos garantizar la formación y apoyo en la lucha contra la ciberdelincuencia, aunque Colombia ya ha obtenido la invitación para pertenecer al Acuerdo, es realmente importante que el país se adhiera para mejorar los resultados en esta lucha, que ya es de carácter global.

En diversas legislaciones del mundo como en Colombia, es a veces imposible judicializar al ciberdelincuente, al no ser encontrados en fragancia o por la falta de denuncias a tiempo, si bien es cierto, que el gobierno ha mantenido un discurso coherente en este tema, también es importante que trabaje en los siguientes aspectos:

1. Garantizar el presupuesto necesario para cumplir con los compromisos que demanda el estar adherido al convenio de ciberdelincuencia de Budapest, no cumpliendo solo con lo básico, sino por el contrario con un porcentaje mayor al establecido. En este punto es vital comprender que la inversión a realizar debe ser muy superior a lo que se tiene planeado, "El presupuesto hasta 2019 será de 85.070 millones de pesos colombianos, unos 28,3 millones de dólares" destinados a la ciberseguridad para los años 2017, 2018 y 2019[87], equivalente a cerca de 9,4 millones de dólares por año; mientras que países como España destinan “20,7 millones de euros para el 2016”[88], cerca de 22.400 millones de dólares con una población aproximada de 45.977.000

[87] SPUTNIK MUNDO, América Latina. Colombia refuerza su presupuesto para planes de seguridad. [Online]. Cuba 2017. [Citado 2017-03-25]. Disponible en internet <https://mundo.sputniknews.com/americalatina/201702021066646346-colombia-ciberseguridad/>

[88] CIBERSEGURIDAD, Al día. INCIBE mantiene su presupuesto en ciberseguridad. [Online]. España: 2016. [Citado 2017-03-25]. Disponible en internet <http://www.ciberseguridadparaempresas.com/incibe-mantiene-su-presupuesto-en-ciberseguridad/>

habitantes[89] y Colombia con 49.068.000[90] habitantes destina mucho menos dinero.

2. El gobierno y las instituciones de defensa deben propender por mejorar la capacitación constante al sistema judicial colombiano, entiéndase como tal Corte Constitucional, Corte Suprema de Justicia, Consejo de Estado, Consejo Superior de la Judicatura, fiscalías, jueces y policía, si bien cierto en abril del 2016 se realizó el lanzamiento de la maestría en ciberdefensa y ciberseguridad en la escuela superior de guerra, es importante tener presente que también se requiere de equipos y redes que permitan realizar prácticas en tiempo real y con objetivos claramente definidos.

3. Deben existir o crear nuevos lugares destinados a controlar, prevenir e investigar los diferentes métodos de cibercrimen, tanto nacionales como internacionales que puedan afectar al pueblo colombiano, si bien es cierto que ya existen algunos (colCERT "Grupo de Respuesta a Emergencias Cibernéticas de Colombia", del CCP "Centro Cibernético Policial" y del CCOC "Comando Conjunto Cibernético"), también es notorio que aún son insuficientes, el estado debe propender porque la capacidad de detección de ataques sea mucho más alta cada día, para lo cual debe tener en cuenta:

    a. Equipos de respuesta basados en la atención e investigación desarrollados en universidades y empresas privadas que puedan ayudar o mejorar procesos.
    b. Contar mínimo con una DMZ externa, uno o varios laboratorios de pruebas los cuales se encuentren aislados evitando el posible daño o afectación a las otras áreas o equipos, contar con al menos 5 zonas como Internet, DMZ externo, DMZ interno, pruebas y la LAN CSIRT.
    c. Personal con conocimientos y capacidades de desarrollar cargos como:
        - ✓ Líderes de equipo
        - ✓ Gestores
        - ✓ Supervisores
        - ✓ HotLine
        - ✓ HelpDesk
        - ✓ Triage
        - ✓ Respuesta a incidentes
        - ✓ Vulnerabilidades
        - ✓ Análisis de equipos
        - ✓ Especialistas

[89] POBLACION, De España. countrymeters. [Online]. España: 2017. [Citado 2017-03-28]. Disponible en internet <http://countrymeters.info/es/España>
[90] POBLACION, De España. countrymeters. [Online]. España: 2017. [Citado 2017-03-28]. Disponible en internet <http://countrymeters.info/es/Colombia>

- ✓ Capacitadores y formadores
- ✓ Desarrollo tecnología
- ✓ control tecnológico

d. Equipos mínimos como servidores de última generación (DNS, Web, correo, intranet, archivos y de monitoreo), equipos portátiles de uso exclusivo laboral, telefonía, Fax, Triturador de papel, dispositivos de almacenamiento lógico de diferentes capacidades y software legal y actualizable en todo momento.[91]

Si bien es cierto que colCERT, CCP y CCOC cuentan con todo ello, también es muy realista el hecho que se debe garantizar al personal, su capacitación, buena remuneración y colaboración, con centros que se deben crear para incentivar una cultura de seguridad informática más fuerte y perdurable, al tener en cuenta que Colombia es un país con aproximadamente 49 millones de habitantes y solo dispone de tres centros especializados para atender todos los casos, es fácil asumir que no alcanza a cumplir con lo presupuestado y debe recurrir a dar prioridad a unos casos sobre otros y evitar la pronta respuesta que se podía dar a algunos de ellos.

4. El gobierno y las universidades deben fortalecer el sistema de educación e investigación en lo referente a las carreras de seguridad informática, técnicas forenses y seguridad en las comunicaciones, con muy altos estándares de calidad, disponiendo de laboratorios y equipos que permitan realizar investigación y prácticas en tiempo real sin afectar a personas o entidades.

5. Al realizar la consulta el SNIES Sistemas información - Ministerio de Educación Nacional, se encontró que actualmente existen siete Programas en pregrado de los cuales uno es técnico, de forma virtual, y seis son tecnologías con metodología presencial y todos ofertados por sector privado. En cuanto al nivel de posgrado, se hallaron 26 programas, de los cuales tres son virtuales, uno a distancia y el resto de forma presencial, de estos últimos, cinco son ofertados por el sector oficial y solo uno existe en la modalidad de Maestría en la especialidad de derecho informático (ver siguiente cuadro).

   Luego, si se tiene en cuenta que en el país existen al 20 de octubre de 2017, 6950 programas con resolución de aprobación vigente y en entidades activas tenemos un 0.37% de programas en posgrado y un 0.1% en nivel tecnológico, las cifras ponen de manifiesto la necesidad de impulsar la formación académica en el ámbito de la seguridad informática, puesto que es prioritario que las instituciones educativas y el Ministerio de Educación,

[91] AMERICANOS, Organización de los estados. Buenas Prácticas para establecer un CSIRT nacional. citado [Online]. Estados Unidos: 2016. [Citado 2017-04-22]. Disponible en internet <https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf>.

comprendan la importancia de tener profesionales que puedan apoyar las labores de investigación y seguridad de la información, a través de capacitación técnica y profesional dentro del país.

Tabla 10 Comparativa estudios en seguridad informática

Tabla 11 (Continuación)

Nombre Institución	Sector	Resolución de Aprobación No.	Fecha de Resolución	Nombre Programa	Metodología	Municipio Oferta
Fundación escuela colombiana de mercadotecnia -ESCOLME-	Privada	4240	19/04/2013	Tecnología en redes y seguridad informática	Presencial	Medellín
Corporación universitaria minuto de dios -UNIMINUTO-	Privada	14244	07/09/2015	Tecnología en gestión de seguridad en redes de computadores	Presencial	Bogotá D.C..
Fundación centro de investigación docencia y consultoría administrativa-f-CIDCA-	Privada	8891	15/07/2013	Tecnología en seguridad informática	Presencial	Bogotá D.C.
Fundación para la educación superior san mateo	Privada	1325	23/02/2011	Tecnología en administración de redes y seguridad informática	Presencial	Bogotá D.C.
Corporación universitaria minuto de dios -UNIMINUTO-	Privada	5359	25/08/2008	Tecnología en redes de computadores y seguridad informática	Presencial	Bogotá D.C.
Politécnico indoamericano	Privada	3791	29/02/2016	Técnico profesional en servicios de seguridad informática	Virtual	Bogotá D.C.
Fundación para la educación superior san mateo	Privada	21985	22/11/2016	Tecnología en administración de redes y seguridad informática	Presencial	Cúcuta
Universidad Externado de Colombia	Privada	63	03/01/2014	Especialización en derecho informático y de las nuevas tecnologías	Presencial	Bogotá D.C.
Fundación universitaria católica del norte	Privada	217	15/01/2013	Especialización en gestión de seguridad y riesgo informático	Virtual	Santa rosa de osos
Dirección nacional de escuelas	Oficial	3268	14/03/2014	Especialización en informática forense	Presencial	Bogotá D.C.
Tecnológico de Antioquia	Oficial	9956	31/07/2013	Especialización en seguridad de la información	Presencial	Medellín

Tabla 11 (Continuación)

Nombre Institución	Sector	Resolución de Aprobación No.	Fecha de Resolución	Nombre Programa	Metodología	Municipio Oferta
Universidad de los andes	Privada	5121	08/11/2005	Especialización en seguridad de la información	Presencial	Bogotá D.C.
Universidad Católica de Colombia	Privada	7471	14/06/2013	Especialización en seguridad de la información	Presencial	Bogotá D.C.
Corporación Universitaria Remington	Privada	6112	06/05/2015	Especialización en seguridad de la información	Presencial	Medellín
Fundación Universitaria CAFAM -UNICAFAM	Privada	2803	16/02/2016	Especialización en seguridad de la información	Presencial	Bogotá D.C.
Politécnico Grancolombiano	Privada	12934	23/09/2013	Especialización en seguridad de la información	Virtual	Bogotá D.C.
Fundación Universitaria Juan de Castellanos	Privada	4632	07/05/2012	Especialización en seguridad de la información	Distancia (tradicional)	Tunja
Universidad Sergio Arboleda	Privada	20216	11/12/2015	Especialización en seguridad de la información e informática	Presencial	Bogotá D.C.
Corporación Universitaria Americana	Privada	10664	09/07/2014	Especialización en seguridad informática	Presencial	Medellín
Corporación Universitaria Americana	Privada	9691	29/07/2013	Especialización en seguridad informática	Presencial	Barranquilla
Corporación Universidad Piloto de Colombia	Privada	16391	18/11/2013	Especialización en seguridad informática	Presencial	Bogotá D.C.
Universidad Autónoma de Occidente	Privada	993	15/02/2011	Especialización en seguridad informática	Presencial	Cali
Universidad Pontificia Bolivariana	Privada	153	16/01/2017	Especialización en seguridad informática	Presencial	Medellín
Universidad Pontificia Bolivariana	Privada	16639	20/11/2013	Especialización en seguridad informática	Presencial	Bucaramanga
Universidad de San Buenaventura	Privada	6060	06/05/2015	Especialización en seguridad informática	Presencial	Medellín
Universidad Nacional Abierta y a Distancia UNAD	Oficial	17195	27/12/2012	Especialización en seguridad informática	Virtual	Bogotá D.C.
Universidad Pontificia Bolivariana	Privada	13932	08/10/2013	Especialización en seguridad informática	Presencial	Bogotá D.C.

Tabla 11 (Continuación)

Nombre Institución	Sector	Resolución de Aprobación No.	Fecha de Resolución	Nombre Programa	Metodología	Municipio Oferta
Fundación Universitaria para el Desarrollo Humano - UNINPAHU	Privada	10429	14/07/2015	Especialización en seguridad informática	Presencial	Bogotá D.C.
Corporación Universitaria de Investigación y Desarrollo - UDI	Privada	7136	22/11/2007	Especialización en seguridad informática	Presencial	Bucaramanga
Corporación Universitaria de Investigación y Desarrollo - UDI	Privada	12314	29/12/2011	Especialización en seguridad informática	Presencial	Barrancabermeja
Escuela Superior de Guerra General Rafael Reyes Prieto	Oficial	2868	06/03/2015	Especialización en seguridad y defensa nacionales	Presencial	Bogotá D.C.
Escuela de Comunicaciones	Oficial	9706	26/07/2013	Especialización seguridad física y de la informática	Presencial	Facatativá

Fuente 24 SNIES https://snies.mineducacion.gov.co/consultasnies/programa

6. Propender por generar una cultura de seguridad informática con muy altos niveles, lo cual permitirá a las empresas y personas del común, comprender a lo que pueden estar expuestos con el uso de las tecnologías de la información, siendo prioritario involucrar a todos los actores.

7. Velar porque los tiempos de respuesta se encuentren dentro de los establecidos en la bilateralidad del convenio para con las otras naciones miembros del convenio de ciberdelincuencia.

8. El gobierno debe tener claridad que la política en lo referente al tema de seguridad informática, debe tratarse con carácter internacional, de dimensiones globales, es vital entender que con la expansión de la tecnología el país puede incurrir en delitos que lleguen a tener afectación en otras jurisdicciones (ciberataques o ciberterrorismo a otras naciones) e involucren a la Corte Penal Internacional.

9. Crear nuevos tratados de extradición que permitan la mejorar de las relaciones internacionales y la cooperación entre países miembros y adheridos al convenio de ciberdelincuencia.

10. Legislar sobre temas aun no regulados como son la ingeniería social, la xenofobia y toda serie de ataques discriminatorios que se generen contra los individuos, a través del uso de internet.

11. Es prioritario que la ley se aplique de forma correcta y basada en los conceptos de especialistas en diferentes áreas, que den garantía sobre la evidencia encontrada para evitar el manto de impunidad que cubre al sistema legal colombiano, por citar, el caso del hacker Sepúlveda, en el que la condena recae sobre el autor material, pero al parecer escatimaron esfuerzos para dar con la aprehensión del autor intelectual.

6. CONCLUSIONES

Durante el desarrollo del proyecto se logró evidenciar que una propuesta integral debe contener la responsabilidad en cuanto a seguridad informática, corresponde a todos los habitantes, por ende, se deben comenzar a gestar campañas educativas que prevenga la configuración de esta clase de delitos tanto a nivel empresarial como individual, de igual forma el gasto en medidas para fortalecer la seguridad informática es considerado de primera importancia, los países no escatiman en equipos, infraestructura y capacitación para poder combatir el flagelo del delito informático, esto se evidencio en la investigación de los países desarrollados, quienes disponen de presupuestos bastante generosos para este gasto.

El trabajo de investigación realizado en lo concerniente al levantamiento de información pone de manifiesto que el convenio de Budapest, es una herramienta jurídica en la cual se pueden apoyar los países que pretendan adherirse, de forma tal, que teniendo como horizonte la legislación interna de cada Estado, lo pueden adaptar con el fin de unir esfuerzos para frenar la ciberdelincuencia, tema en el cual Colombia ya tiene avances significativos.

En comparación a los otros países en proceso de adhesión al Convenio de Ciberdelincuencia de Budapest, Colombia ha realizado muy grandes esfuerzos para legislar, reglamentar y tratar de pertenecer al convenio, es prioritario que no desfallezca en tan importante tarea actualizado constantemente la legislación sobre lo que pueda faltar o mejorar.

En cuanto al nivel de capacitación en Colombia sobre el tema de seguridad informática, aún es escaso, se requiere de un mayor esfuerzo y dedicación por parte de las instituciones educativas, privadas y públicas, a fin de promover y fortalecerse la investigación en esta área de conocimiento de forma que permita los cumplimientos de adhesión al tratado de ciberdelincuencia de Budapest.

7. RECOMENDACIONES

La investigación evidencia la necesidad del fortalecimiento de todas las instituciones a través de la capacitación y la compra o mejora de equipos que permitan aumentar la seguridad informática a nivel organizacional.

La investigación demostró la necesidad de aumentar la capacitación en seguridad informática, esta debe ser uno de los principales estandartes de las políticas universitarias y gubernamentales.

Se recomienda a los jueces y legisladores que la correcta aplicación de la ley debe ser primordial al momento de tratarse de un delito de carácter informático, evitando la ambigüedad o privilegios por el nivel de estudios que pueda o no tener una persona.

Los CERT, CCIRT, Jueces, expertos en Seguridad Informática y entes judiciales deben tener presente que el delito informático está en constante evolución, lo cual debe ocasionar que la reformulación de la legislación y sus diferentes aplicaciones sea constantemente necesaria.

Se recomienda al estado colombiano que los tratados de extradición deben ser revisados y contemplar siempre la posibilidad de ser aplicados a delincuentes informáticos tanto a nivel intelectual como material.

De acuerdo a los hallazgos encontrados en la investigación, se recomienda que el Gobierno y/o los Honorables representantes del Congreso de la República, presenten y discutan proyectos de Ley dirigidos a regular temas como la ingeniería social, xenofobia y toda clase de discriminación que atente contra la dignidad del ser humano a través del uso de la internet, de forma que pueda generar pautas para un futuro.

8. BIBLIOGRAFÍA

AMERICANOS, Organización de los estados. Buenas Prácticas para establecer un CSIRT nacional. citado [Online]. Estados Unidos: 2016. [Citado 2017-04-22]. Disponible en internet <https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf>.

AUSTRALIAN, Government Atorney-General's Department. www.ag.gov.au, Cyber security. [Online]. Australia: 2016- [citado 2016-11-20]. Disponible en internet <https://www.ag.gov.au/RightsAndProtections/CyberSecurity/Pages/default.aspx>.

AUSTRALIAN, Government. Federal Register of Legislation. Cybercrime Act 2001. [Online]. Australia: se2016. [Citado 2016-11-20]. Disponible en internet <https://www.legislation.gov.au/Details/C2004A00937>.

AUSTRALIAN, Government. Informe 2015 Cyber Security Survey. Major Australian Businesses. Australian Cyber Security Centre: 2015. Pág. 24

AUSTRALIAN, Government. Institute of Criminology. Cybercrime, Cybercrime in focus. [Online]. Australia: 2015. [Citado 2016-11-20]. Disponible en internet <http://www.aic.gov.au/crime_types/in_focus/cybercrime.html>.

AZNAR, A. La red Internet. El modelo TCP/IP. Madrid: 2005 Grupo Abantos formación y consultoría. Pág. 61

BID, Banco Interamericano de Desarrollo. Informe de Ciberseguridad. [Online]. Observatorio de la ciberseguridad en América Latina y el caribe: 2016. [Citado 2016-11-20]. Disponible en internet <http://observatoriociberseguridad.com/graph/countries//selected//0/dimensions/1-2-3-4-5>.

BRIGADA DE INVESTIGACIÓN TECNOLÓGICA, Policía Española. [Online]. España: 2015. [Citado 2016-12-20]. Disponible en internet <http://delitosinformaticos.info/delitos_informaticos/tipos_delitos.html>.

CALDWELL, Leslie. justice.gov, Department Releases Intake and Charging Policy for Computer Crime Matters. [Online]. Estados Unidos: 2016- [citado 2016-11-20]. Disponible en internet <https://www.justice.gov/opa/blog/department-releases-intake-and-charging-policy-computer-crime-matters>.

CANADA, Government. Canada and the Council of Europe. [Online]. Canadá: 2015. [Citado 2016-11-20]. Disponible en internet <http://www.canadainternational.gc.ca/eu-ue/bilateral_relations_bilaterales/council_europe_conseil.aspx?lang=eng>.

CANADA, Government of. Justice Laws Website, Criminal Code (R.S.C., 1985, c. C-46). [Online]. Canadá: 2016. [Citado 2016-11-20]. Disponible en internet <http://laws-lois.justice.gc.ca/eng/acts/c-46/index.html>.

CANADA, Statistics. Police-reported cybercrime in Canada, 2012. [Online]. Canadá: 2012. [Citado 2016-11-20]. Disponible en internet <http://www.statcan.gc.ca/pub/85-002-x/2014001/article/14093-eng.htm>.

CIBERSEGURIDAD, Al día. INCIBE mantiene su presupuesto en ciberseguridad. [Online]. España: 2016. [Citado 2017-03-25]. Disponible en internet <http://www.ciberseguridadparaempresas.com/incibe-mantiene-su-presupuesto-en-ciberseguridad/>

COBB, Stephen. Welivesecurity, Cybercrime in Canada: The impact on SMBs. [Online]. Canadá: 2016- [citado 2016-11-20]. Disponible en internet <http://www.welivesecurity.com/2016/10/10/cybercrime-in-canada-the-impact-on-smbs/>

COLOMBIA, MINISTERIO DE COMUNICACIONES. Decreto 1524 de 2002. (30, julio, 2002). El cual reglamenta el artículo 5o. de la Ley 679 de 2001 referente a Pornografía en menores de edad. [En línea]. <http://www.icbf.gov.co/cargues/avance/docs/decreto_1524_2002.htm> [citado en 7 de noviembre 2016]

COLOMBIA, CONGRESO DE LA REPUBLICA. Ley Estatutaria 1266. (31, diciembre, 2008). Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países. [En línea]. <https://www.bancoldex.com/documentos/1291_Ley_1266_de_2008_(Habeas_Data).pdf> [citado en 7 de noviembre 2016]

COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 527 de 1999. (18, agosto, 1999). Por la cual se definen y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación. [En línea]. <http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/LEY_527_DE_1999.pdf> [citado en 7 de octubre 2016]

COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 599 de 2000. (24, julio, 2000). Por la cual se Expide el Código Penal. En esta se mantuvo la estructura del tipo penal de “violación ilícita de comunicaciones”, se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. [En línea]. <http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html> [citado en 7 de noviembre 2016]

COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1273 de 2009. (05, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. [En línea]. <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492> [citado en 17 de noviembre 2016]

COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1336 de 2009. (21, julio, 2009). Por la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes. [En línea]. <http://www.anato.org/sites/default/files/Ley1336de2009.pdf> [citado en 17 de noviembre 2016]

COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1341 de 2009. (30, julio, 2009). Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones - TIC-, se crea la agencia nacional del espectro y se dictan otras disposiciones. [En línea]. <http://www.mintic.gov.co/portal/604/articles-3707_documento.pdf> [citado en 7 de noviembre 2016]

COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1581 de 2012. (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. [En línea]. <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981> [citado en 7 de octubre 2016]

COUNCIL OF EUROPE, General information. Participation of Non-member States. [Online]. Estrasburgo: 2016. [Citado 2016-11-20]. Disponible en internet <http://www.coe.int/en/web/conventions/participation-of-non-member-states>.

CONSEJO DE EUROPA, Serie de tratados europeos. Convenio sobre la Ciberdelincuencia. [Online]. Budapest: 2001. [Citado 2016-11-20]. Disponible en internet <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41c>.

EDITOR, El economista. Colombia es referente mundial en la lucha contra la ciberdelincuencia. [Online]. Colombia 2016- [citado 2016-11-20]. Disponible en internet <http://www.eleconomistaamerica.co/telecomunicacion-tecnologia-co/noticias/7946347/11/16/Colombia-es-referente-mundial-en-la-lucha-contra-la-ciberdelincuencia.html>

ELHANEM, Elhanem. Espacio libre dentro de los límites de lo posible, Los delitos cibernéticos. Cara fea de la TI. [Online]. Israel: 2016. [Citado 2016-11-20]. Disponible en internet < https://elhanem.wordpress.com/جرائم-الانترنت-الوجه-القبيح-للتكنولو>.

EL NACIONAL, República Dominicana. Líderes de telecomunicaciones plantean a expertos extranjeros situación de ciberseguridad en RD. [Online]. República Dominicana: 2016. [Citado 2016-11-20]. Disponible en internet <http://elnacional.com.do/lideres-de-telecomunicaciones-plantean-a-expertos-extranjeros-situacion-de-ciberseguridad-en-rd/>.

EFE, Agencia. Australia anuncia una estrategia de ciberseguridad frente a ataques cibernéticos. [Online]. España: 2016- [citado 2016-11-20]. Disponible en internet <http://www.efe.com/efe/espana/portada/australia-anuncia-una-estrategia-de-ciberseguridad-frente-a-ataques-ciberneticos/10010-2903210>.

ESCRIVA Gascó, Gema, Romero Serrano, Rosa María, and Ramada, David Jorge. Seguridad informática. Madrid, ES: Macmillan Iberia, S.A., 2013.

ESPAÑA, Gobierno de. Informe Análisis de derecho comparado sobre ciberdelincuencia, ciberterrorismo y ciberamenzas al menor. España: 2015. Pág. 581

ESPAÑA, Ministerio de asuntos exteriores y cooperación. Consejo de Europa, Historia y actividad del Consejo de Europa. [Online]. España: 2016. [Citado 2016-11-20]. Disponible en internet <http://www.exteriores.gob.es/portal/es/politicaexteriorcooperacion/consejodeeuropa/paginas/historiaactividadconsejoeuropa.aspx>.

EUROPE. Council of. Explanatory Report to the Convention on Cybercrime, European Treaty Series - No. 185. [Online]. Budapest: 2001. [Citado 2016-11-20]. Disponible en internet

<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b>.

FLOREZ, Lucerito. Derecho informático. México: Grupo editorial patria. 2014. Pág. 24

GOMEZ. Álvaro. Auditoría de seguridad informática. Madrid, ES: RA-MA Editorial, 2014.

GUISARRE, Carlos. revistaitnow.com, ¿Qué hace República Dominicana para fortalecer ley contra el cibercrimen? [Online]. Centro América y Caribe: 2015- [citado 2016-11-20]. Disponible en internet <https://revistaitnow.com/ley-contra-el-ciberdelito-debe-ser-mas-clara-en-republica-dominicana/>.

INTERNATIONAL MCCONNELL. Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information. Washington, DC: 2011. [En línea]. Disponible desde internet:
<http://www.iwar.org.uk/law/resources/cybercrime/mcconnell/CyberCrime.pdf>

JACKSCH, Eric. itincanadaonline, The magnitude of the cybercrime problem. [Online]. Canadá: 2016- [citado 2016-11-20]. Disponible en internet <http://www.itincanadaonline.ca/index.php/columnists/eric-jacksch/1882-the-magnitude-of-the-cybercrime-problem>.

KASPERSKY, Security. Moscú: 2015. Pág. 85

KESSEM, Limmor. securityintelligence.com, Organized Cybercrime Big in Japan: URLZone Now on the Scene. [Online]. Estados Unidos: 2016- [citado 2016-11-20]. Disponible en internet <https://securityintelligence.com/organized-cybercrime-big-in-japan-urlzone-now-on-the-scene/>.

KHAN, Zak. cso.com.au, Australia, we need to talk about cybercrime. [Online]. Australia: 2016- [citado 2016-11-20]. Disponible en internet <http://www.cso.com.au/article/599457/australia-we-need-talk-about-cybercrime/>.

KIM, Michael. ¿Cómo manejan los países los delitos informáticos? [Online]. Estados Unidos: 1997. [Citado 2016-11-20]. Disponible en internet <http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall97-papers/kim-crime.html>.

LA PRENSA, Política. Acechan delitos informáticos. [Online]. Panamá: 2015. [Citado 2016-11-20]. Disponible en internet <http://www.prensa.com/politica/Acechan-delitos-informaticos-Panama_0_4220578020.html>

MACEDO, Maximiliano; TEMPERINI, Marcelo y BORGHELLO, Cristian. Reporte ODILA (Observatorio de Delitos Informáticos de Latinoamérica) 2016. Pág. 20

MITZNER, Dennis. InfoWorld, Israeli cybertech startups set global security trends. [Online]. Jerusalén: 2016- [citado 2016-11-20]. Disponible en internet <http://www.infoworld.com/article/3032213/cyberwarfare/israeli-cybertech-startups-set-global-security-trends.html>.

MORALES, Thalia S. Acechan los delitos informáticos en Panamá. [Online]. Panamá: 2015. [Citado 2016-11-20]. Disponible en internet <http://www.prensa.com/politica/Acechan-delitos-informaticos-Panama_0_4220578020.html>.

MEDERO, Gema. Ciberespacio y el crimen organizado. 2012. Revista Enfoques. Pág. 20

MEDINA, Edgar. El tiempo. Tecnosfera, En 2015, cibercrimen generó pérdidas por US$ 600 millones en Colombia. [Online]. Colombia: 2015. [Citado 2016-11-17]. Disponible en internet <http://www.eltiempo.com/tecnosfera/tutoriales-tecnologia/cuantos-delitos-informaticos-se-denuncian-en-colombia/16493604>.

MINTIC, Ministerio de Tecnologías, Información y Comunicaciones. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. 2016 [citado 2017-10-10]. Disponible en internet <https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf>.

NAVEGANTE TECNOLOGIA, El mundo.es Japón aprueba una ley que criminaliza la creación de virus informáticos. [Online]. España: 2011. [Citado 2016-11-20]. Disponible en internet <http://www.elmundo.es/elmundo/2011/06/17/navegante/1308304867.html>.

PAGNOTTA, Sabrina. Welivesecurity Noticias, opiniones y análisis de la comunidad de seguridad de ESET, Top 5 de las brechas de datos más devastadoras de 2015. [Online]. Latinoamérica: 2016. [Citado 2016-11-20]. Disponible en internet <http://www.welivesecurity.com/la-es/2016/01/08/top-5-brechas-de-datos-devastadoras-2015/>.

PANAMA, Departamento de cooperación Jurídica. Derecho Sustantivo. [Online]. Panamá: 2016. [Citado 2016-11-20]. Disponible en internet <http://www.oas.org/juridico/spanish/cyb_pan.htm>.

PREES, Europa. España se suma a la propuesta, Treinta países firman la primera Convención Internacional contra el 'Cibercrimen'. [En línea]. España: 2001. [Citado

2016-11-20]. Disponible en internet <http://www.elmundo.es/navegante/2001/11/26/esociedad/1006766268.html>.

POBLACION, De España. countrymeters. [Online]. España: 2017. [Citado 2017-03-28]. Disponible en internet <http://countrymeters.info/es/España>

POBLACION, De España. countrymeters. [Online]. España: 2017. [Citado 2017-03-28]. Disponible en internet <http://countrymeters.info/es/Colombia>

PORTAL COUNCIL OF EUROPE. Acerca de los tratados [en línea]. <http://www.coe.int/en/web/conventions/about-treaties> [citado en 5 de octubre 2016]

PORTAL, Council of Europe. Parties/Observers to the Budapest Convention and Observer Organizations to the T-CY. [Online]. Council of Europe: 2017. [Citado 2016-11-20]. Disponible en internet <http://www.coe.int/en/web/cybercrime/parties-observers>.

REPUBLICA DE COLOMBIA, Consejo Nacional de Política Económica y Social. CONPES 3701(14, julio, 2011). Lineamientos de política para ciberseguridad y ciberdefensa. [En línea]. <http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf> [citado en 17 de noviembre 2016]

REPUBLICA DE COLOMBIA, Consejo Nacional de Política Económica y Social. CONPES 3854 (11, abril, 2016). Política nacional de seguridad digital. [En línea]. <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf> [citado en 17 de noviembre 2016]

SPUTNIK MUNDO, América Latina. Colombia refuerza su presupuesto para planes de seguridad. [Online]. Cuba 2017. [Citado 2017-03-25]. Disponible en internet <https://mundo.sputniknews.com/americalatina/201702021066646346-colombia-ciberseguridad/>

Anexo A Resumen analítico en educación - RAE

Universidad Nacional Abierta y a Distancia	**FORMATO**
	RESUMEN ANALÍTICO EN EDUCACIÓN - RAE
Código: 001	**Versión: 01**
Fecha de Aprobación: 16-05-2017	**Página 172 de 177**

1.Información General	
Tipo de documento	Trabajo de grado.
Acceso al documento	Universidad Nacional Abierta y a Distancia.
Título del documento	Estudio de una adhesión de Colombia al convenio de Budapest, visto desde la legislación y seguridad informática
Autor(es)	William Martínez Camargo
Director	Manuel Antonio Sierra Rodríguez, Salomón González,
Publicación	Bogotá, Universidad Nacional Abierta y a Distancia, 2017. 177 p.
Unidad Patrocinante	Ninguna
Palabras Claves	Convenio de ciberdelincuencia de Budapest, legislación informática, Ley 1273 de 2009, Ciberdelincuencia, Ciberdelito, Ciberdefensa, Ciberespacio, Ciberterrorismo.

2.Descripción
Monografía - Estudio de una adhesión de Colombia al convenio de Budapest, visto desde la legislación y seguridad informática. para optar al título de Especialista en seguridad informática.

3.Fuentes
117 fuentes bibliográficas entre libros, revistas, portales y consultas a páginas gubernamentales.

4.Contenidos

El mundo nunca antes ha sido tan tecnológico y es mucho lo que espera a las nuevas generaciones en esta materia, los países crecen de forma desigual, pero la tecnología no tiene presente esto, el afán por vender y consumir todo tipo de aparatos tecnológicos deja al descubierto la gran necesidad de capacitación sobre seguridad informática. Con el desmesurado avance en la creación de nueva tecnología aparecieron palabras como ciberdelito, ciberdelincuencia, ciberdefensa y tantas otras que lo único que nos hace pensar es que el mundo evoluciona de forma más dinámica y que cada segundo que pasa, el planeta entero se expone a un mayor riesgo, surgen preguntas como: ¿Es tal vez el momento de que el mundo entero se una para hacer frente a la gran amenaza del ciberdelito?, ¿Realmente necesita Colombia pertenecer al convenio de ciberdelincuencia de Budapest?, ¿Necesita el país realizar grandes cambios para lograr una verdadera adhesión al convenio de ciberseguridad de Budapest?

El presente documento recoge la investigación realizada sobre el convenio de Ciberdelincuencia de Budapest, entre los cuales se evidencian los antecedentes, el marco jurídico existente del mismo, los actores del convenio, su normatividad y tendencias; en lo concerniente a Colombia realiza una revisión de la legislación en materia de seguridad informática, el estado actual, sus falencias y necesidades a futuro.

El alcance del documento es el de generar una propuesta para la adhesión de Colombia al convenio en ciberdelincuencia de Budapest, por esta razón el estudio parte de una contextualización y estudio de las diferentes variables, escenarios que se ven y verán comprometidos en el marco de una eventual adhesión al convenio.

Colombia viene trabajando desde hace ya varios años en materia de seguridad informática, ciberdelincuencia y ciberdefensa, muestra de ello es la elaboración de legislación al respecto, entre la cual está la Ley 527 de 1999, Ley 299 de 2000, Ley 962 de 2005, Ley 1341 de 2009 y muchas otras, que serán vistas en el texto, al igual que el documento CONPES 3701 del año 2011. Sin embargo, es imperativo comprender que al adherirse a un tratado de carácter internacional Colombia tendrá que cumplir con una cantidad de requisitos en materia legislativa y contar con determinados recursos. Es muy importante que el pueblo comprenda la importancia, derechos, deberes y demás que este tipo de adhesiones trae para el país, por esta razón un documento que ilustre a todos es de carácter vital.

El convenio de Budapest o de ciberdelincuencia como es más conocido, fue establecido cuando ya existían otros convenios de cooperación en Europa en materia penal, partiendo de la necesidad de unir esfuerzos para la lucha contra los delitos de carácter informático en el continente europeo, conto con la presencia de países observadores como Canadá, China y Japón de los cuales posteriormente se adhirió Canadá y Japón, en la actualidad se espera que países como Costa Rica, Chile, Uruguay, Colombia y otros tengan la posibilidad.

En cuanto a legislación se aclara que el Convenio de ciberdelincuencia da unas pautas o guía para que cada país legisle de forma integral y acorde a sus preceptos dentro de lo que su constitución o carta magna les permita de forma que pueda llegar a ser vinculante a un marco de cooperación internacional, ya sea como estado adherido o como parte del mismo convenio.

El convenio de ciberdelincuencia de Budapest, está enmarcado dentro de los convenios celebrados dentro del consejo de Europa, es un tratado de carácter internacional, por tal razón está cubierto por todos los derechos de los tratados de la convención de Viena de 1969.

Por otra parte, Colombia ha progresado en la legislación informática, sin embargo, en materia de seguridad su situación durante el año 2015 fue 7.118 denuncias 40% más que en el 2014, un incremento en más del 50% en amenazas cibernéticas, 4.572 (64%) casos fueron hurtos por medios informáticos, 1.087 (15.27%) casos de abusos de sistemas informáticos en total generaron más de 600 millones de pesos en pérdidas durante el año 2015 según fuente MEDINA, Edgar. El tiempo. Tecnosfera, 2015. Y las Nuevas tendencias en ciberdelincuencia están apareciendo todo el tiempo, ocasionando costos muy altos a la economía mundial, los cuales se cuentan en miles de millones de dólares.

En el pasado, el delito cibernético era cometido principalmente por individuos o grupos pequeños, sin embargo, hoy en día, se ven complejas redes cibercriminales que actúan por todo el mundo, reclutando personas de diferentes nacionalidades, esto demuestra que la delincuencia informática es cada vez más evolucionada en cuanto a organización sea dicho, además se está sumando el ciberterrorismo auspiciado por grupos tan fuertes como el Estado Islámico, ISIS y también por los mismos gobiernos.

Pertenecer al convenio de ciberdelincuencia de Budapest puede resultar ser muy importante en materia de colaboración internacional, capacitación y lucha contra la delincuencia informática en todas sus formas, sin embargo, se debe tener muy presente los requerimientos al momento de comenzar a formar parte del convenio.

El país requiere realizar mayor inversión de capital, el sistema legislativo requiere ser endurecido y mejorado, los sistemas de denuncias y la información referente a la ciberdelincuencia deben ser más accesibles y fáciles de realizar, se deben crear mecanismos que permitan realizar un adecuado tratamiento de los impactos sufridos por la ciberdelincuencia, el estado debe comprometerse con destinar un buen capital para la realización de la estrategia de seguridad informática a nivel nacional.

Por otra parte, hay que tener en cuenta que por muchos esfuerzos que se realicen el no pertenecer a este convenio limita las posibilidades del país en el evento de solicitar apoyo o capacitación sobre esta temática, es innegable el hecho de que Colombia no tiene la capacidad financiera suficiente para estar a la altura de

países como Estados Unidos, Reino Unido, China, Israel o Rusia que destinan grandes cantidades de capital a combatir la ciberdelincuencia.

Sin la adhesión al convenio el país debe invertir más dinero en capacitación de sus diferentes centros de reacción.

5.Metodología

Investigación de carácter Bibliográfico y documental, basada en la recolección, selección y análisis de documentos, utilizando procedimientos de carácter lógico y mental como el análisis, síntesis, deducción e inducción que permitirán la generación de una nueva propuesta a través de la presentación de resultados.

Se toma como base los conocimientos y criterios correspondientes al convenio de ciberdelincuencia, la seguridad informática y parámetros legislativos en Colombia y la unión europea al igual que en los países adheridos.

El desarrollo de toda investigación conlleva un plan detallado y pormenorizado, de la siguiente forma:

- Levantamiento de información y generación de conceptualización
- Generación de antecedentes que permitan mostrar al lector el camino que llevo al convenio de Budapest, su creación, variables que le dieron adhesión a los países miembros, y países adheridos brindando una tipificación de estos.
- Presentación del estado actual de los países adheridos y Colombia.
- Elaboración y determinación de la proyección a futuro.
- Tendencias de hacia donde nosotros podemos dirigirnos, en la posibilidad de adherirnos acorde a lo que les ha pasado a los otros países.
- Análisis y elaboración de la propuesta.

Para cumplir con los objetivos y el plan diseñado se realizará consulta bibliográfica a través de documentos físicos y electrónicos como:

- Libros: Consultados directamente en bibliotecas como la Luis Ángel Arango, Julio Mario Santo Domingo, Virgilio Barco y en internet a través de la biblioteca virtual de la Universidad Nacional Abierta y a Distancia UNAD.
- Publicaciones Periódicas: Como jurisprudencia, leyes, normas.
- Documentos electrónicos: Consultas en internet alusivas a revistas, periódicos, artículos científicos de Bases de datos, Documentos oficiales y portales como el del Consejo de Europa.

Al finalizar la consulta y registro de información se procederá al análisis documental de forma objetiva extrayendo la información necesaria para poder realizar la comparación, análisis crítico, resúmenes y generación de la propuesta que permita brindar conocimiento y valor agregado a todo aquel que la consulte.

materiales utilizados: consulta bibliográfica, documentos online, material de biblioteca, artículos, revistas, documentos oficiales, normas legales, software office, etc.

6.Conclusiones

1. Durante el desarrollo del proyecto se logró evidenciar que una propuesta integral debe contener la responsabilidad en cuanto a seguridad informática, corresponde a todos los habitantes, por ende, se deben comenzar a gestar campañas educativas que prevenga la configuración de esta clase de delitos tanto a nivel empresarial como de individual, de igual forma el gasto en medidas para fortalecer la seguridad informática es considerado de primera importancia, los países no escatiman en equipos, infraestructura y capacitación para poder combatir el flagelo del delito informático, esto se evidencio en la investigación de los países desarrollados, quienes disponen de presupuestos bastante generoso para este gasto.
2. El trabajo de investigación realizado en lo concerniente al levantamiento de información pone de manifiesto que el convenio de Budapest, es una herramienta jurídica en la cual se pueden apoyar los países que pretendan adherirse, de forma tal, que teniendo como horizonte la legislación interna de cada Estado, lo pueden adaptar con el fin de unir esfuerzos para frenar la ciberdelincuencia, tema en el cual Colombia ya tiene avances significativos.
3. En comparación a los otros países en proceso de adhesión al Convenio de Ciberdelincuencia de Budapest, Colombia ha realizado muy grandes esfuerzos para legislar, reglamentar y tratar de pertenecer al convenio, es prioritario que no desfallezca en tan importante tarea actualizado constantemente la legislación sobre lo que pueda faltar o mejorar.
4. En cuanto al nivel de capacitación en Colombia sobre el tema de seguridad informática, aún es escaso, se requiere de un mayor esfuerzo y dedicación por parte de las instituciones educativas, privadas y públicas, a fin de promover y fortalecerse la investigación en esta área de conocimiento de forma que permita los cumplimientos de adhesión al tratado de ciberdelincuencia de Budapest.

Elaborado por:	William Martínez Camargo
Revisado por:	Francisco Nicolás Javier Solarte y Martin Camilo Cancelado Tuiz

Fecha de elaboración del Resumen:	28	11	2017