IMPLICACIONES DE LA SEGURIDAD INFORMÁTICA EN LA LEGISLACIÓN COLOMBIANA

SANDRA MILENA HERNÁNDEZ LUNA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

MANIZALES, CALDAS

2018

IMPLICACIONES DE LA SEGURIDAD INFORMÁTICA EN LA LEGISLACIÓN COLOMBIANA

SANDRA MILENA HERNANDEZ LUNA

MONOGRAFÍA

DIRECTOR

ALEXANDER LARRAHONDO NÚÑEZ

DOCENTE ESP. EN SEGURIDAD INFORMÁTICA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

MANIZALES, CALDAS

2018

Nota de Aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Ciudad y fecha

DEDICATORIA O LEMA

“Creo que los virus informáticos deberían contar como vida. Creo que dice bastante sobre nosotros el hecho de que la única forma de vida que hemos logrado crear sea puramente destructiva. Hemos creado vida basada en nuestra imagen.”

Stephen Hawking

AGRADECIMIENTOS

A Dios.

Por darme vida y salud para llegar hasta este punto.

A mi Familia.

Por las palabras de aliento que me llenaron de motivación para continuar con mis estudios a pesar de los obstáculos presentados en el camino.

Docentes y Asesores de la UNAD.

Por el acompañamiento y disposición para el desarrollo de este documento.

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

LISTA DE TABLAS

pág.

INTRODUCCIÓN

En un mundo globalizado y que cada vez implementa la tecnología para el desarrollo de los procesos industriales, económicos, financieros y muchos más, generando grandes beneficios tanto para las empresas como para la sociedad en general, es necesario implementar leyes que regulen el acceso a los sistemas de información y en general todos aquellos comportamientos que busquen afectar a uno o varios individuos haciendo uso de las redes de información.

Cada vez aumenta el número de suscriptores al Internet, lo cual ha traído grandes beneficiarios para estos, pero a su vez se han desarrollado nuevas prácticas delincuenciales las cuales, a pesar de ser denunciadas por las víctimas, los procesos se tardan demasiado en ser investigados y en muchas ocasiones no se logran resolver.

El presente documento expone la manera como se espera contribuir a la comunidad por medio de una propuesta que integra conocimientos legales y procedimentales de la seguridad informática.

1. PLANTEAMIENTO DEL PROBLEMA

¿Se conocen las implicaciones legales de la seguridad informática en Colombia?

La legislación informática en Colombia es un tema que aún se puede llamar terreno desconocido para muchos profesionales en el área del Derecho, son pocos los asesores en esta rama que cuenten con especializaciones relacionadas con la seguridad informática y posean las habilidades técnicas como lo puede ser salvaguardar una evidencia digital correctamente y que esta pueda ser tomada como prueba válida en un tribunal.

Aunado a lo anterior, la desinformación de los usuarios de las redes sociales frente a la publicación de información personal y/o sensible ha conllevado a que se presente una gran cantidad de situaciones no deseadas y que a futuro se generen problemas sociales, económicos, emocionales, laborales, entre otros. No es un secreto que la proliferación de los delitos informáticos no solo en el país sino a nivel mundial crece de una manera exponencial, pero en la mayoría de casos la raíz del problema radica en la falta de cultura informática lo que genera un impacto negativo en la sociedad. De allí se generaría un interrogante: ¿Se conocen las implicaciones legales de la seguridad informática en Colombia?

2. JUSTIFICACION

La falta de cultura informática de la sociedad en general sumado a la escasez de profesionales en la rama del Derecho que cuenten con la formación necesaria en el área de Seguridad Informática en Colombia, es la problemática que conlleva a justificar el desarrollo de la presente monografía; en la cual se desea contribuir a la sociedad recopilando los métodos mediante los cuales se puede integrar la normatividad vigente Colombiana con la investigación del delito informático utilizando los procedimientos técnicos necesarios de la Ingeniería Forense.

Así mismo, teniendo en cuenta la problemática expuesta anteriormente se darán a conocer las diferencias existentes entre los delitos clásicos que utilizan como medio la tecnología y aquellos que se tipifican como delitos informáticos en Colombia, la manera de diferenciarlos toda vez que en algunos casos se pueden confundir teniendo en cuenta que el común denominador para llevar a cabo cualquiera de ellos siempre será a través del uso de la tecnología.

Brindar un recurso de fácil consulta por medio del cual las personas identifiquen aquellos elementos que deben tener presente cuando se genere un delito, diferenciación y pasos a seguir en este tipo de acciones que se generen.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Identificar la importancia de la legislación vigente en seguridad informática en Colombia y las consideraciones necesarias a la hora de denunciar un delito informático.

3.2 OBJETIVOS ESPECIFICOS

- ✓ Mostrar la legislación vigente en temas de seguridad informática aplicada en el contexto colombiano (intrusión, acceso no autorizado, ley 1581, ley delitos informáticos, características punitivas, tiempos de condena, sentencias de la corte).

- ✓ Estudiar el proceso de custodia de las evidencias forenses en la investigación de los delitos informáticos en el país.

- ✓ Considerar la importancia de la sensibilización en el uso de las tecnologías partiendo del principio de prevención de posibles situaciones.

4. MARCO CONCEPTUAL Y TEORICO

La ley 1273 de 2009 la cual establece "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"; es expedida en Colombia en respuesta al incremento exponencial a nivel mundial de los ataques perpetrados por delincuentes cibernéticos que acceden sin autorización a una red, servidor o sistema informático para causar daño.

La gran dificultad para descubrir y enfrentar a los involucrados en este tipo de actos hace necesario que no solo Colombia, sino que varios países dispusieran de un sistema judicial especializado para hacer frente a este fenómeno que trae consigo el auge de las tecnologías.

Así mismo, se han establecido tratados internacionales y que surgen debido al mal uso de la tecnología. La Organización Mundial del Comercio (OMC): En su artículo 61 establece que "Para los casos de falsificación dolosa de marcas de fábrica o de comercio o de piratería lesiva del derecho de autor a escala comercial se establecerán procedimientos y sanciones penales además de que los recursos disponibles comprenderán la pena de prisión y/o la imposición de sanciones pecuniarias suficientemente disuasorias". Cabe mencionar que uno de los delitos más comunes en Colombia es la violación a los derechos de autor.

La LPI (Ley de Propiedad Intelectual) la cual regula los derechos de autor en los medios digitales, estableciendo que la reproducción digital de un medio debe realizarse bajo la autorización del titular del contenido.

A continuación, se mencionan algunos convenios internacionales:

El Convenio de Berna para la protección de las obras literarias y artísticas.

La convención sobre la Propiedad Intelectual de Estocolmo

La Convención para la Protección y Producción de Fonogramas de 1971

La Convención Relativa a la Distribución de Programas y Señales.

Desde los años ochenta se han venido realizando y promoviendo una serie de estudios a nivel mundial con el fin de hacer posible la creación y unificación de la

legislación para la comisión de los delitos informáticos, desde la Organización de Cooperación y Desarrollo Económico OCDE, la cual indicó en el año 1983 que el principal problema es la falta de leyes unificadas lo cual facilita la comisión de los delitos.

En el año 1992 la OCDE elaboró un marco normativo y se recomendaron algunos ejemplos de uso indebido con el fin de que los países tuvieran el conocimiento de qué tipo de delitos prohibir y sancionar con leyes penales; en 1991 la ONU publica una descripción de tipos de delitos informáticos; en 1992 La Asociación Internacional de Derecho Penal adoptó diversas recomendaciones respecto a los delitos informáticos, entre ellas que, en la medida que el derecho Penal no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos.

La Ley Orgánica de Protección de Datos de Carácter Personal aprobada por las Cortes Generales el 13/12/1999, establece las bases para proteger el tratamiento de los datos de carácter personal que se encuentren ya sea en medios digitalizados o físicos.

La ley de servicios de la Sociedad de Información y Comercio Electrónico (LSSI-CE del 11/07/2002) y principalmente busca regular los portales web que utilizan el comercio electrónico ya sea para pago de cuotas, venta de productos y/o servicios; estableciendo que dichos portales deben incluir información visible en la página donde se visualice la información de la empresa o persona, NIT, dirección, entre otros, que den cuenta de quién se encuentra detrás de la página.

Es importante resaltar que en el proceso legislativo no solamente es necesaria la aplicación de las leyes nacionales, teniendo en cuenta, además; que las nuevas tecnologías que emergen cada día deberán estar reguladas por una legislación transnacional por lo que sería conveniente que entre países se pudieran establecer acuerdos y de esta manera se definan leyes comunes frente a estas nuevas tecnologías.

La continua evolución de la tecnología hace que sea necesario utilizar medios jurídicos prácticos y eficaces para prevenir los riesgos que conlleva; los esquemas jurídicos tradicionales deben ser replanteados y rediseñados periódicamente de acuerdo a las nuevas figuras delictivas, así mismo la importancia de la formación y especialización por parte de los jueces, fiscales, organismos de policía judicial de nuestro país con el fin de que se obtengan adecuadas respuestas legales y

judiciales frente a este tipo de delitos, pues todo apunta a que la tecnología avanza mucho más rápido que la legislación, encontrando una salida por parte de los criminales quienes se aprovechan de esta situación.

Colombia, es uno de los países que cuenta con la legislación más clara frente al tema de los delitos informáticos según Alexander Díaz García, Juez Segundo de control de garantías de Róvira (Tolima) y especialista en nuevas tecnologías y protección de datos. Así mismo Díaz García resalta la importancia de saber diferenciar entre delito informático y delito clásico a través de medios electrónicos, toda vez que el primero se refiere a la vulneración de la información y el dato privado mientras que el delito clásico informático se refiere al ilícito consumado a través de medios electrónicos. Estas diferencias aún no son conocidas por muchos jueces y abogados en el país por lo que muchas veces se desconoce la manera como se deben juzgar este tipo de delitos.

Es muy importante que los organismos judiciales reciban la capacitación necesaria en materia de sensibilización y apropiación de los sistemas de información toda vez que aún en el tema digital y jurídico hay bastante tela por cortar.

La organización Symantec es una multinacional estadounidense desarrolladora y comercializadora de software especialmente en Seguridad Informática. Symantec anualmente realiza una publicación con el escalafón de los países que presentaron mayor número de ataques. En el informe del año 2017 Symantec analizó 157 países donde se situó a Colombia como el sexto país con mayor número de ataques cibernéticos.

A nivel laboral el blanco de los ciberdelincuentes han sido las entidades financieras por razones económicas obvias como el secuestro de información, con el auge del internet de las cosas se abren nuevas fronteras y retos en el tema de seguridad informática, se genera un interrogante ¿a quién le interesaría hackear mi reloj inteligente, mi vehículo o mi nevera?; algunos de estos contienen información sensible, en el caso de los automóviles ya se ha demostrado que es posible tomar control de estos por medio de la red, generando choques o robo de autos, para el caso de los electrodomésticos se pueden convertir en puertas de entrada para atacar otros aparatos o saltar a una casa vecina para tomar control de sus aparatos domésticos; además teniendo en cuenta que los electrodomésticos no presentan actualizaciones en el software pues básicamente su diseño impera en la durabilidad del aparato.

Otros casos que se han presentado mucho más delicados y que pueden llegar a costar la vida de una persona son aquellos dispositivos diseñados por industrias tecnológicamente avanzadas y que son implantados en el cuerpo humano para suplir el funcionamiento de un órgano vital como el caso de un marcapasos, respiradores, entre otros; los cuales pueden al igual que cualquier otro aparato conectado a la red ser el blanco de un ataque. Este es el caso de un Malware que fue infiltrado en el marcapasos de una investigadora llamada Marie Moe, quien compartió su experiencia durante una Conferencia Internacional de Ciberseguridad donde indicó que su marcapasos a la edad de 20 años empezó a funcionar como si tuviera 60 años de edad; finalmente se descubrió que un gusano cibernético o malware lo había infectado y era el causante de su mal funcionamiento.

Siendo uno de los países donde se presenta gran cantidad de ataques cibernéticos es indispensable que en primer lugar se reconozca que el usuario es el mejor sistema de protección con que se puede contar, partiendo de esto la importancia de sensibilizar a los usuarios del internet frente a que la seguridad no solo es cuestión de antivirus y configuraciones en las redes y computadores sino de ser cuidadosos y cautelosos a la hora de ejecutar programas desconocidos, abrir correos electrónicos llamativos y descargar archivos.

En un ejemplo común comparar el comportamiento que se tiene en la red con aquel que se tiene dentro de una vivienda, afirmando que cuando una persona se encuentra dentro de una vivienda, chequeará antes de abrir la puerta con el fin de asegurarse de que la persona que está afuera es confiable, y no accederá a brindar información a un desconocido; igualmente cuando un individuo camina por la calle es cauteloso de no ser perseguido o trata de identificar algún tipo de patrón extraño en el comportamiento de otra persona. Es importante asemejar este comportamiento mientras una persona se encuentra conectada al internet desde cualquier dispositivo, al realizar la publicación de una foto en una red social, esta se almacenará en una gran cantidad de servidores y aunque sea eliminada por el usuario quedará alojada en algún dispositivo desconocido para él.

Es imposible no utilizar la tecnología para socializar con otros individuos, especialmente aquellas aplicaciones de mensajería instantánea, redes sociales, para mantenernos en contacto unos con otros; conocer nuevas personas inclusive a miles de kilómetros de distancia, ampliar ese círculo de amistad que sin la tecnología seguramente sería mucho más limitado; pero es allí; en este punto donde las personas deben comprender la importancia de ser cautos y desconfiados con nuestras relaciones de amistad, amorosas, laborales, las cuales como pueden perdurar en el tiempo puede que se rompan en algún momento y es allí donde aquellos mensajes enviados con fotos y videos personales corren el riesgo de ser publicados con el propósito de causar algún tipo de daño a la persona involucrada.

Miles de personas han sido víctimas en el mundo de la porno venganza, personas famosas y comunes han sido grabadas por sus parejas ya sea con o sin su consentimiento en videos sexuales los cuales posteriormente son publicados en internet, algunos de estos son subastados especialmente para el caso de personas reconocidas en el medio.

Teniendo en cuenta lo anterior, como Especialista en Seguridad Informática se espera profundizar en el tema de la legislación informática como un complemento clave para adquirir el conocimiento, el cual permita ser de apoyo a la sociedad frente a un tema que se volvió parte de la rutina diaria pero que presenta aun muchos vacíos, en una relación que se podría denominar como ciber-legislación. La sociedad depende cada vez más del uso de las tecnologías para realizar sus actividades, por lo que será necesario utilizar los medios jurídicos para prevenir ser víctimas de ataques, pero esto conlleva también a la aplicación de diversos procedimientos tecnológicos que incluyan el uso correcto de las herramientas tecnológicas que permitan recolectar las evidencias necesarias y bajo los procedimientos legales establecidos.

5. CRONOGRAMA DE DESARROLLO

Tabla 1. Cronograma de Desarrollo

Actividad	Mes I	Mes II	Mes III	Mes IV	Mes V	Mes VI	Mes VII	Mes VIII	Mes IX	Mes X	Mes XI	Mes XII
Reconocimiento Opciones de Grado	X											
Lluvia de ideas		X										
Selección de Propuesta		X	X									
Título de Propuesta			X									
Resumen				X								
Planteamiento del Problema					X							
Justificación						X						
Objetivo General							X					
Objetivos Esp.							X					
Marco Conceptual y Teórico								X	X			
Evaluar Propuesta Desarrollo opción de Grado										X	X	X

Fuente: Autor.

6. CAPITULO I

MOSTRAR LA LEGISLACIÓN VIGENTE EN TEMAS DE SEGURIDAD INFORMÁTICA APLICADAS EN EL CONTEXTO COLOMBIANO (INTRUSIÓN, ACCESO NO AUTORIZADO, LEY 1581 DE 2012, LEY 1273 DE 2009 DE DELITOS INFORMÁTICOS, CARACTERÍSTICAS PUNITIVAS, TIEMPOS DE CONDENA, SENTENCIAS DE LA CORTE).

6.1 Ley 1273 de 2009

En Colombia la respuesta legal y judicial frente a la comisión de delitos informáticos por parte de Juzgados y tribunales ha sido encaminada hacía el clásico Derecho Penal, generando poca coherencia y precisión al momento de clasificar diferentes tipos de acciones informáticas ilícitas o conductas asociadas a estas.

Debido a la necesidad de un ajuste legislativo correcto a la problemática generada en la sociedad, frente al uso de los sistemas informáticos, al auge del comercio electrónico, los dispositivos de almacenamiento de datos, las comunicaciones en línea, entre otros elementos, los cuales, a pesar de facilitar y agilizar significativamente los procesos industriales, laborales, educativos, científicos, médicos, entre otros; también han sido generadores de una serie de comportamientos ilícitos. De allí se promulga en Colombia la 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 los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

La ley 1273 de 2009 incorpora nuevas figuras delictivas relacionadas directamente con los aspectos informáticos o afines con las nuevas tecnologías de la información, con el objetivo de ofrecer una respuesta coherente y precisa frente a aquellas acciones informáticas ilícitas, pero no sin dejar atrás el enfoque tradicional del Derecho penal.

A continuación, se detallan de una manera clara los artículos correspondientes de la ley mencionada:

Tabla 2. Ley 1273 de 2009.

	De los Atentados Contra la Confidencialidad, la Integridad, la Disponibilidad de los Datos y de los Sistemas Informáticos			
Artículo	**Descripción**	**Sentencia de la Corte**	**Tiempo de Condena**	**Multa**
Artículo 269A: Acceso Abusivo a un Sistema Informático.	Acceder a un sistema informático protegido o que utilice medidas de seguridad sin autorización o en contra de la voluntad de a quien legalmente le pertenezca.	Prisión y Multa	48 a 96 meses	100 a 1000 SMLV
Artículo 269B: Obstaculización Ilegítima de Sistema Informático o Red de Telecomunicación	Quien, sin estar facultado, impida u obstaculice el funcionamiento o acceso normal a un sistema informático, sus datos o red de telecomunicación.	Prisión y Multa	48 a 96 meses	100 a 1000 SMLV
Artículo 269C: Interceptación de Datos Informáticos	Quien sin orden judicial previa intercepte datos informáticos en su origen, destino o al interior de un sistema informático, o las emisiones electromagnéticas provenientes del el mismo.	Prisión	36 a 72 meses	N.A

Tabla 2. (Continuación)

Artículo 269D: Daño Informático	Quien, sin estar facultado, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos.	Prisión y Multa	48 a 96 meses	100 a 1000 SMLV
Artículo 269E: Uso de Software Malicioso	Quien, 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.	Prisión y Muta	48 a 96 meses	100 a 1000 SMLV
Artículo 269F: Violación de Datos Personales	Quien, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique, emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o dios semejantes.	Prisión y Multa	48 a 96 meses	100 a 1000 SMLV

Tabla 2. (Continuación)

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. Además, quien modifique el sistema de resolución de nombres de dominio con el fin de hacer entrar al usuario a una IP diferente a la que se cree.	Prisión y Multa	48 a 96 meses	100 a 1000 SMLV

Circunstancias de agravación punitiva	
Artículo	**Descripción**
Artículo 269H: Circunstancias de Agravación Punitiva	Las penas mencionadas en los artículos descritos anteriormente se aumentarán de la mitad a las tres cuartas partes si se cometiere: 1. Sobre redes o sistemas informáticos estatales u oficiales o del sector financiero, nacionales o extranjeros. 2. Por servidor público en ejercicio de sus funciones 3. Aprovechando la confianza depositada en el poseedor de la información o por quien tuviere un vínculo contractual con este. 4. Revelando o dando a conocer información en perjuicio de otro. 5. Obteniendo provecho para sí o 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 dichas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta tres años, la pena de inhabilitación para el ejercicio de la profesión relacionada con los sistemas de información procesada con equipos computacionales.

Tabla 2. (Continuación)

De los Atentados Informáticos y Otras Infracciones				
Artículo	**Descripción**	**Sentencia de la Corte**	**Tiempo de Condena**	**Multa**
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.	Prisión. (Incurrirá en las penas señaladas en el artículo 240 del código penal).	5 a 12 años	N.A
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.	Prisión y multa	48 a 120 meses	200 a 1500 SMLV

6.2 Ley 1581 de 2012

El 17 de octubre de 2012 se expide en Colombia la ley estatutaria 1581 de 2012, la cual tiene como objetivo proteger la información o datos personales que se encuentran almacenados y sean tratados u operados por parte de empresas públicas o privadas.

Se establece el Habeas Data como un derecho fundamental dado que la información personal pertenece a la vida privada y familiar de un individuo y sobre la cual ni el estado ni las empresas pueden interferir.

Todas las personas tienen el derecho a conocer la información que sobre ellas se ha almacenado en las bases de datos, así mismo la autorización de acceder a esta donde sea que se encuentre guardada, además tienen el derecho de actualizar la información para contar con información que se ajuste a la realidad del momento, así mismo el titular puede solicitar la corrección de datos errados y si lo desea solicitar la exclusión de información de una base de datos ya sea porque evidencie el uso indebido de esta o porque simplemente sea su voluntad, esta última presenta algunas excepciones que se encuentran señaladas en la normatividad.

6.2.1 Clasificación de los datos

- ✓ Dato personal público: Datos que no son semiprivados o privados como: documentos públicos, sentencias judiciales, estado civil de las personas.
- ✓ Dato personal semiprivado: Dato que no tiene naturaleza íntima y que puede interesar no solo al titular sino a la sociedad en general, grupo o sector de personas como: historial crediticio, datos financieros, reporte eb centrales de riesgo.
- ✓ Dato personal privado: Dato íntimo o reservado que solo puede interesar al titular del dato como: correo electrónico, teléfono, dirección residencia, fotografías o videos que expongan un estilo de vida.

- ✓ Dato personal sensible: Dato que puede afectar la intimidad de una persona o en caso de uso indebido le cause a esta discriminación sea por su religión, orientación sexual, política, ideología, estado de salud, entre otros.

El incumplimiento de la ley dará lugar a las sanciones respectivas para los responsables del tratamiento o encargados del tratamiento de los datos personales.

6.2.2 Sanciones

- ✓ Multa de carácter personal e institucional hasta por dos mil (2.000) SMLV al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó.

- ✓ Suspensión de actividades relacionadas con el tratamiento por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deben adoptar.

- ✓ Cierre temporal de las actividades relacionadas con el tratamiento una vez culminado el término de suspensión sin que se hubiere adoptado los correctivos que se deberán adoptar.

- ✓ Cierre inmediato y definitivo de la operación que involucre el tratamiento de datos sensibles.

Las sanciones mencionadas anteriormente solo aplican para las personas de naturaleza privada, en los casos que la Superintendencia de Industria y Comercio advierta presunto incumplimiento de una autoridad pública a las disposiciones de la ley mencionada, se remitirá la actuación a la Procuraduría General de la Nación para que se adelante la investigación correspondiente.

El Artículo 24 establece algunos criterios para graduar las sanciones.

6.2.2.1 Grado de la sanción

- ✓ La dimensión del daño o peligro a los intereses jurídicos tutelados por la presente ley.
- ✓ El beneficio económico obtenido por el infractor o terceros, en virtud de la comisión de la infracción.
- ✓ La reincidencia en la comisión de la infracción.
- ✓ La resistencia, negativa u obstrucción a la acción investigadora o de vigilancia de la Superintendencia de Industria y Comercio.
- ✓ La renuencia o desacato a cumplir las órdenes impartidas por la Superintendencia de Industria y Comercio.
- ✓ 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.

6.3 Ley 1341 de 2009

Es la ley 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 de Espectro y se dictan otras disposiciones.

El objeto de la Ley 1341 de 2009 es crear un marco general para formular políticas públicas que rijan es sector de las Tecnologías de la Información y las Telecomunicaciones, como su ordenamiento general, régimen de competencia, protección al usuario, cobertura, calidad del servicio, inversión en el sector de las tecnologías, uso eficiente de redes y del espectro radioeléctrico. En general esta ley se crea como una política de estado teniendo en cuenta que las tecnologías de la información deben servir al interés general y el estado tiene el deber de promover su acceso eficiente y en igualdad de oportunidades a todos los habitantes del país.

6.3.1 Principios Orientadores

- ✓ Prioridad al acceso y uso de las tecnologías de la información.
- ✓ Libre competencia.
- ✓ Uso eficiente de la infraestructura y de los recursos escasos.
- ✓ Protección de los derechos de los usuarios.
- ✓ Promoción de la inversión.
- ✓ Neutralidad Tecnológica.
- ✓ Derecho a la comunicación, la información y la educación y los servicios básicos de las TIC.
- ✓ Masificación del Gobierno en Línea.

El artículo 65 establece sanciones a personas naturales o jurídicas que incurran en las infracciones señaladas en el artículo 64 de la presente ley y las cuales mencionamos a continuación.

6.3.2 Sanciones

- ✓ No respetar la confidencialidad o reserva de las comunicaciones.
- ✓ Proveer redes y servicios o realizar telecomunicaciones en forma distinta a lo previsto en la ley.
- ✓ Utilizar el espectro radioeléctrico sin el correspondiente permiso o en forma distinta a las condiciones de su asignación.
- ✓ El incumplimiento de las obligaciones derivadas de las concesiones, licencias, autorizaciones y permisos.
- ✓ Abstenerse de presentar a las autoridades la información requerida o presentarla de forma inexacta o incompleta.

- ✓ Incumplir el pago de las contraprestaciones previstas en la ley.
- ✓ Incumplir el régimen de acceso, uso, homologación e interconexión de redes.
- ✓ Realizar subsidios cruzados o no adoptar contabilidad separada.
- ✓ Incumplir los parámetros de calidad y eficiencia que expida la Comisión de Regulación de Comunicaciones (CRC).
- ✓ Violar el régimen de inhabilidades, incompatibilidades y prohibiciones previsto en la ley.
- ✓ La modificación unilateral de parámetros técnicos esenciales y el incumplimiento de los fines del servicio de radiodifusión sonora.
- ✓ Cualquiera otra forma de incumplimiento o violación de las disposiciones legales, reglamentarias o contractuales o regulatorias en materia de telecomunicaciones.
- ✓ Cualquier práctica o aplicación que afecte negativamente el medio ambiente, en especial el entorno de los usuarios, el espectro electromagnético y las garantías de los demás proveedores y operadores y la salud pública.

6.3.2.1 Criterios e imposición de sanciones

- ✓ Amonestación.
- ✓ Multa hasta por 2000 SMLV.
- ✓ Suspensión de la operación al público hasta por 2 meses
- ✓ Caducidad del contrato o cancelación de la licencia, autorización o permiso.

Los criterios para la definición de las sanciones son:

- ✓ La gravedad de la falta.
- ✓ Daño producido.

- ✓ Reincidencia en la comisión de los hechos.
- ✓ Proporcionalidad entre la falta y sanción.

Las normas y leyes que se aplican en el mundo digital son una labor de cada estado, toda vez que no existen unas políticas uniformes y estandarizadas que regulen todos los países frente al Internet y su uso.

6.4 Realidades de Intrusión, Acceso No Autorizado y Delito Informático en Colombia.

El pasado 10 de abril de 2018 se generó la condena más alta en Colombia por delitos informáticos, esta condena le fue impartida a Andres Fernando Sepúlveda Ardila en el caso conocido como “Hacker Sepúlveda”; quien fue contratado en el año 2014 como asesor en redes sociales y seguridad informática por el excandidato presidencial Oscar Iván Zuluaga.

La condena de 10 años de prisión (luego realizar preacuerdo con la Fiscalía y colaborar con entrega de información) y multa de 120 smlmv fue impartida por los delitos de:

- ✓ Acceso abusivo a un sistema de información.
- ✓ Violación de datos personales agravado.
- ✓ Uso de software malicioso.
- ✓ Violación ilícita de comunicaciones.
- ✓ Espionaje y concierto para delinquir.

Además, Andrés Sepúlveda llevó a cabo las siguientes acciones ilícitas:

- ✓ Interceptación de correos electrónicos del presidente Juan Manual Santos y su secretaria privada a través del uso de software para el acceso a la información.

- ✓ Publicación de datos de carácter reservado sobre miembros de las FARC con el objetivo de sabotear el proceso de paz.

- ✓ Compra de información militar sobre desmovilizados de las FARC y obtención de correos electrónicos de directivos de grupos armados ilegales.

- ✓ Logró identificar cada uno de los guerrilleros desmovilizados y reinsertados a la vida civil.

- ✓ Interceptación de la Policía Nacional y el Comité Operativo para la Dejación de Armas del Ministerio del Interior.

En las actividades ilegales ejecutadas desde la oficina del Hacker Andrés Sepulveda se suman otros capturados, algunos de ellos se encuentran libres o en proceso de recuperar su libertad.

Uno de los capturados fue Daniel Bajaña Barragán, hacker ecuatoriano condenado a prisión de 3 años 4 meses por realizar seguimientos electrónicos ilegales al ex vicepresidente Francisco Santos y quien actualmente se encuentra libre y declaró insolvencia para pagar la multa impuesta por el juez que lo sentenció.

Otros fueron capturados por vender información reservada a Sepúlveda y de los cuales algunos se encontraban vinculados a la Dirección Nacional de Inteligencia (DNI), Central de Inteligencia Técnica del Ejército (CITEC) y Policía de Bogotá.

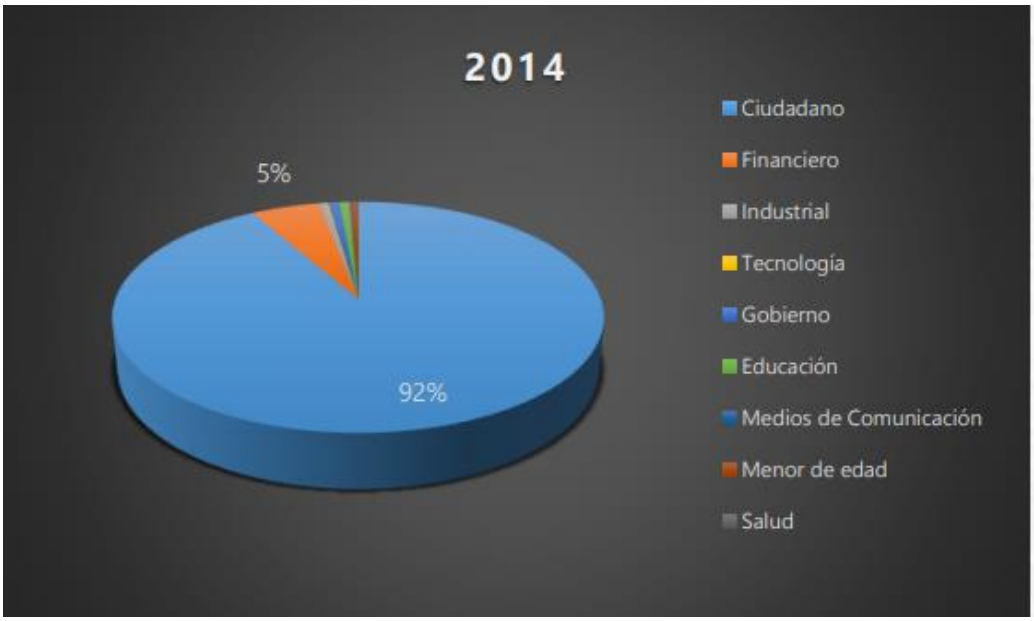
6.5 Estadística - Delitos Informáticos en Colombia.

El Centro Cibernético de la Policía Nacional y la Cámara Colombiana de Informática y Telecomunicaciones publicaron en el año 2017 el primer Informe denominado “Amenazas del Cibercrímen en Colombia 2016-2017”. El informe presentado expone una recopilación de estadísticas criminales que desde el año 2014 se han venido incrementando en el país.

Entre al año 2014 y 2017, se evidencia que año tras año la selección de víctimas por parte de los ciberdelincuentes ha presentado transformaciones, teniendo en

cuenta que en el año 2014 el objetivo se centraba especialmente en atacar a los ciudadanos del común con un promedio del 92% como lo muestra la siguiente gráfica:

Figura 1. Estadística Víctimas 2014- Sectores



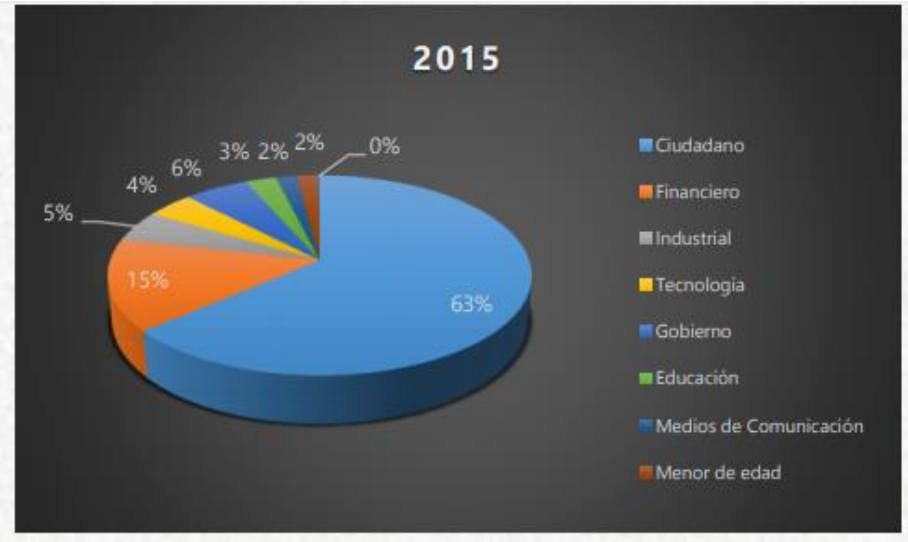
Centro Cibernético Policial. Amenazas del cibercrimen en Colombia 2016 – 2017. [En línea]. Colombia. [Consultado marzo de 2017]. Disponible en internet: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

Para el año 2015 esta cifra se reduce a un 63% y para el 2016 disminuye aún más con un 57% de ataques a ciudadanos del común; pero a su vez se presenta un incremento del 5% a un 28% los ataques realizados al sector empresarial.

Lo anterior confirma el planteamiento realizado por la IOCTA (Internet Organised Crime Threat Assessment) del European Law Enforcement Agency EUROPOL, quienes refieren el término Tricotomía del Delito, el cual consiste en realizar ataques mucho más especializados a sectores reducidos y con mayores niveles de seguridad como lo es el sector financiero, puesto que al lanzar ataques que requieren de mayor habilidad e innovación representa un beneficio económico

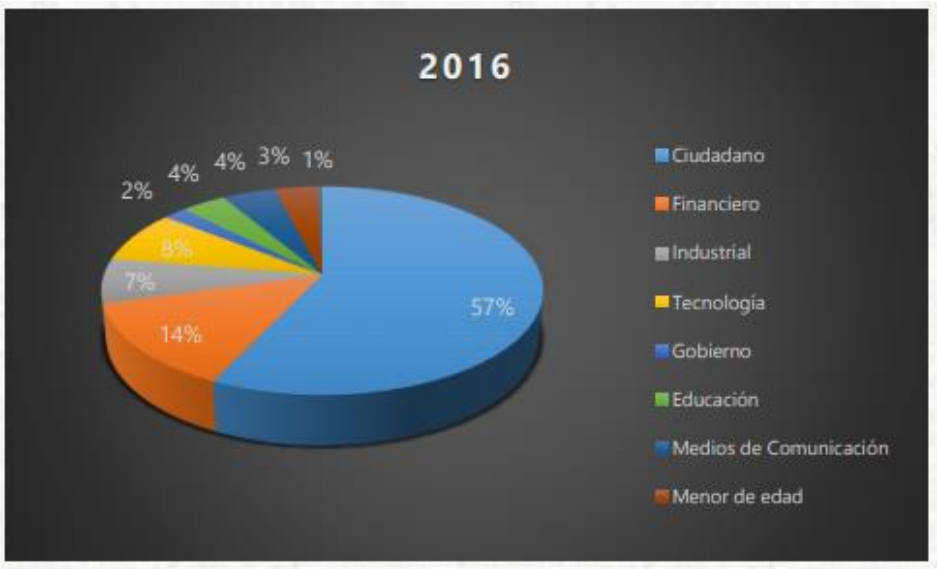
mucho más alto que al realizar ataques a un mayor número de víctimas con niveles bajos de protección en los cuales se obtienen pocos beneficios.

Figura 2. Estadística Víctimas 2015- Sectores



Centro Cibernético Policial. Amenazas del cibercrimen en Colombia 2016 – 2017. [En línea]. Colombia. [Consultado marzo de 2017]. Disponible en internet: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

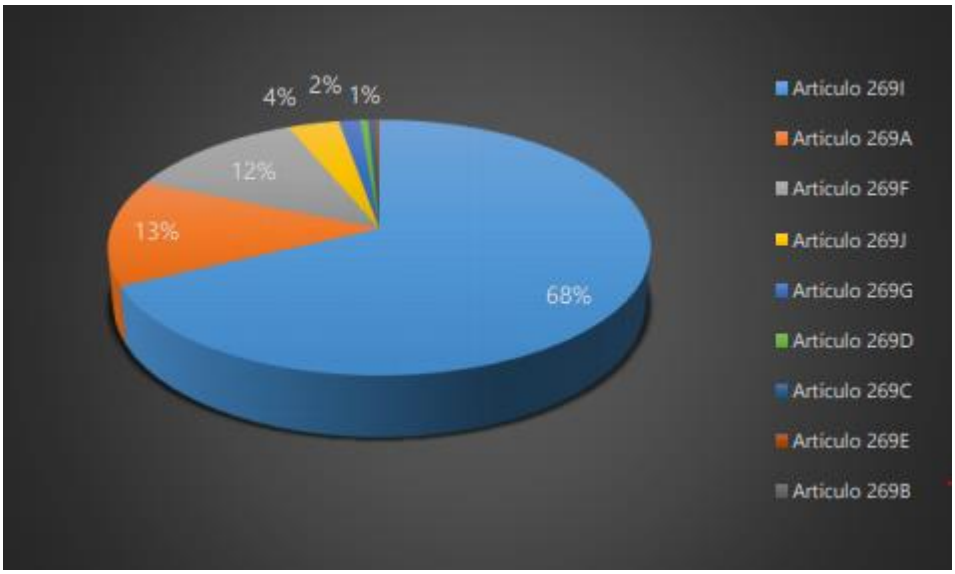
Figura 3. Estadística Víctimas 2016- Sectores



Centro Cibernético Policial. Amenazas del cibercrimen en Colombia 2016 – 2017. [En línea]. Colombia. [Consultado marzo de 2017]. Disponible en internet: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

Los tres principales delitos que han sido denunciados en el país entre el periodo 2014-2017 son: Hurto por medios informáticos y semejantes, Acceso Abusivo a un sistema informático y Violación de Datos personales. A continuación, se observa el porcentaje de denuncias realizadas por violación de la ley 1273 de 2009, donde en el periodo mencionado anteriormente se presentaron 13.774 denuncias.

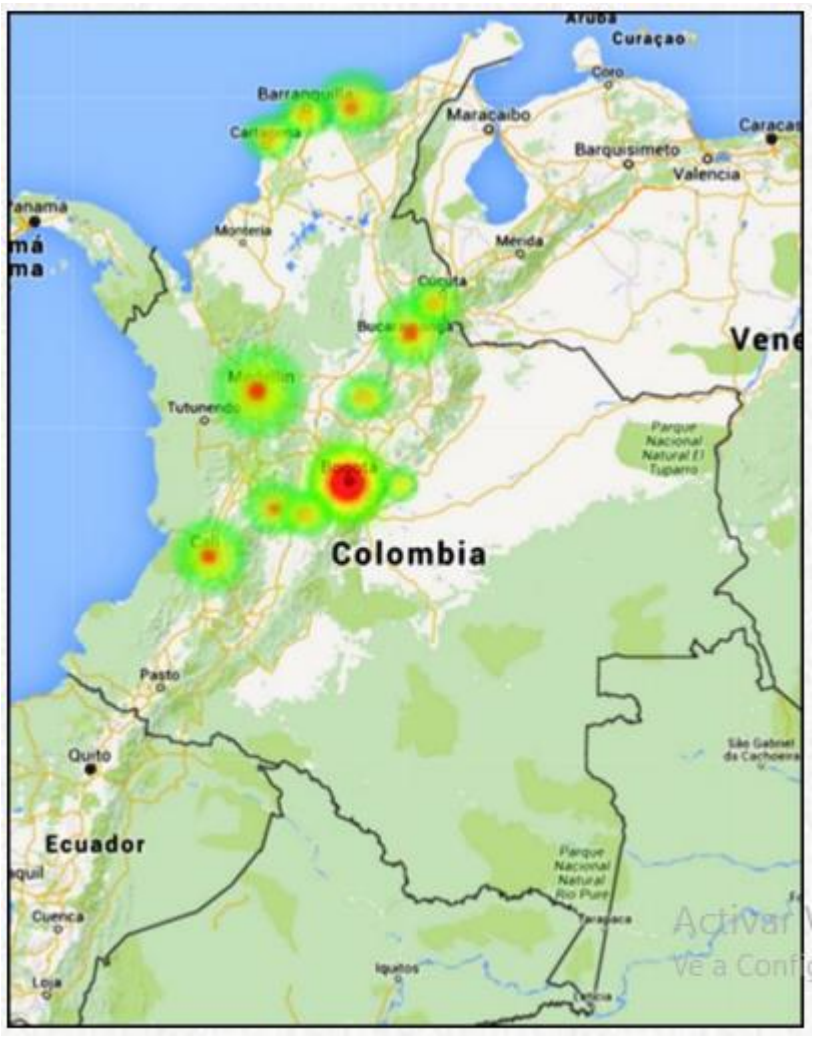
Figura 4. Estadística Víctimas 2017- Sectores



Centro Cibernético Policial. Amenazas del cibercrimen en Colombia 2016 – 2017. [En línea]. Colombia. [Consultado marzo de 2017]. Disponible en internet: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

El informe presentado por el Centro Cibernético Policial expone las ciudades del país en las cuales se presentó mayor cantidad de denuncias relacionadas con la ley 1273 de 2009 entre el año 2014 y 2017, siendo Bogotá, Cali, Medellín, Bucaramanga, Ibagué y Barranquilla, además teniendo en cuenta que estas ciudades presentan mayor índice de habitantes por ciudad en Colombia y la mayor cantidad de suscriptores a internet. Mapa de calor del ciberdelito:

Figura 5. Mapa de Calor - Delito Informático.



Centro Cibernético Policial. Amenazas del cibercrimen en Colombia 2016 – 2017. [En línea]. Colombia. [Consultado marzo de 2017]. Disponible en internet: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

Para el 2018 la Fiscalía General de la Nación presenta 17.898 registros de las noticias criminales en el Sistema Penal Oral Acusatorio (SPOA) por presuntos hechos delictivos conocidos por el ente gubernamental a partir de la entrada en vigencia de la Ley 906 de 2004 y la Ley 1098 de 2006.

Con el fin de conocer las estadísticas relacionadas con delitos informáticos se descarga el archivo de extensión .csv denominado Victimas Spoa 2018, el cual a diferencia que las estadísticas gráficas y las cuales no se encuentran disponibles en la página web de la Fiscalía contienen unas variables adicionales, permitiendo el procesamiento de la información en una hoja de cálculo Excel, generar tabla

dinámica para el manejo de la información y exponerla de la siguiente manera para una mayor comprensión del lector.

La siguiente tabla expone el número de casos tipificados como “De la protección de la información y datos”, por tipo de Noticia recibida (Actos urgentes, Asistencia judicial, Compulsación de copias, de oficio, Denuncia, Petición especial y Querella), su estado, ya sea Activo o Inactivo y la Etapa procesal en que se encuentran.

Se observa que la Denuncia es el tipo de noticia que presenta mayor número de reportes, con un total de 17.523 de casos, de los cuales 13.344 se encuentran activos a corte 10 de enero de 2019.

Tabla 3. Victimas SPOA 2018

Tipo Noticia/ Delito/Estado	Ejecución de Penas	Indagación	Investigación	Juicio	Querellable	Terminación Anticipada	Total General
Actos Urgentes	14	68	5	24	1	4	116
De la Protección de La Información y de los Datos	14	68	5	24	1	4	116
Activo	4	61	4	24	1	4	98
Inactivo	10	7	1				18
Asistencia Judicial		1					1
De la Protección de La Información y de los Datos		1					1
Activo		1					1
Compulsación De Copias	5	27	2	8			42
De la Protección de La Información y de los Datos	5	27	2	8			42
Activo		25	2	8			35
Inactivo	5	2					7
De Oficio (Informes)	8	65	11	29	1		114

Tabla 3. (Continuación)

Tipo Noticia/ Delito/Estado	Ejecución de Penas	Indagación	Investigación	Juicio	Querellable	Terminación Anticipada	Total General
De la Protección de La Información y de los Datos	8	65	11	29	1		114
Activo	1	59	11	29	1		101
Inactivo	7	6					13
Denuncia	37	17278	34	80	92	2	17523
De la Protección de La Información y de los Datos	37	17278	34	80	92	2	17523
Activo	1	13168	32	77	65	1	13344
Inactivo	36	4110	2	3	27	1	4179
Petición Especial		6					6
De la Protección de la Información y de dos Datos		6					6
Activo		6					6
Querella		32			64		96
De la Protección de La Información y de los Datos		32			64		96
Activo		18			53		71
Inactivo		14			11		25
Total General	**64**	**17477**	**52**	**141**	**158**	**6**	**17.898**

Realizando un paralelo entre la cifra de denuncias recibidas entre los años 2014 – 2017 por violación a la ley 1273 de 2009 a nivel país con 13.774 denuncias y que expone el Informe generado por el Centro Cibernético Policial Vs los casos reportados como Denuncia solo en el año 2018 (17.523) y que expone el sitio web de la Fiscalía General de la Nación en su sección “Datos abiertos” se evidencia un incremento significativo, toda vez que en un solo año se generaron más denuncias que entre el 2014 al 2017.

Lo anterior responde al auge en el uso del internet que cada año gana mayor cantidad de usuarios, presentándose un incremento en la criminalidad, reflejados en situaciones como pornografía infantil, redes de lavado, búsqueda de víctimas, robo de dinero por medio de pago digital, tarjeta de crédito o más conocido como carding, violación de datos personales y muchos otros delitos informáticos.

Aún la sociedad desconoce el fenómeno de la criminalidad cibernética, por lo tanto, es de gran importancia que los gobiernos nacionales establezcan estrategias que impacten realmente y sensibilicen a usuarios del común y organizaciones públicas y privadas para protegerse de esta realidad que cada día crece y seguirá en aumento teniendo en cuenta los avances tecnológicos que llevarán a enfrentar nuevos desafíos como lo es el uso del internet de las cosas.

7. CAPITULO II

ESTUDIAR EL PROCESO DE CUSTODIA DE LAS EVIDENCIAS FORENSES EN LA INVESTIGACION DE LOS DELITOS INFORMÁTICOS EN EL PAÍS.

7.1 Antecedentes

El Ministerio de las Tecnologías de la Información y las Telecomunicaciones desarrolló y publicó la Guía # 13 para Evidencias Digitales en el documento Seguridad y Privacidad de la Información a través de la estrategia Gobierno en Línea. En este capítulo se referencian los procedimientos establecidos en la guía, teniendo en cuenta que esta se encuentra dirigida a las entidades públicas de orden nacional y territorial, proveedores de servicio de Gobierno en Línea y particulares que se interesen en aplicar los Lineamientos del modelo de Seguridad y Privacidad de la Información para Evidencias Digitales.

Teniendo en cuenta lo anterior, es necesario que los profesionales del áreas relacionadas con la Seguridad Informática se familiaricen y estén en la capacidad de aplicar el Modelo de Seguridad y Privacidad de la Información enmarcado en la estrategia Gobierno en Línea tomando como base los lineamientos recomendados por la ISO IEC 27001 para 2013 para llevar a cabo una correcta identificación, recolección, análisis y manipulación de información luego de presentarse un incidente de seguridad que requiera ser investigado.

7.2 Incidentes de seguridad

En el momento que se genera un evento relacionado con la Seguridad de la información es importante identificar si este evento clasifica como un Incidente de Seguridad de la Información o si por el contrario no se debe iniciar ningún procedimiento investigativo. Para ello, consultar la Guía # 25 denominada “Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información”, incluida en el modelo de Seguridad y Privacidad de la Información, disponible en https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf.

Cada entidad es responsable de definir su propia clasificación de incidentes de seguridad de la información, de acuerdo a su infraestructura, riesgos y criticidad de los activos, por lo tanto, no existe un estándar de clasificación de riesgos que pueda

ser usado por todas las organizaciones, sin embargo, a continuación, se mencionan algunos ejemplos de elementos como son:

- ✓ Acceso no autorizado: Incidente que implica a un individuo, sistema o código malicioso que accede sin autorización del propietario a una aplicación, sistema o activo de información.

- ✓ Modificación de recursos no autorizado: Incidente que implica a un individuo, sistema o código malicioso que afecta la integridad de la información o de un sistema informático.

- ✓ No disponibilidad de los recursos: Incidente que implica a un individuo, sistema o código malicioso que imposibilita el uso autorizado de un activo de información.

- ✓ Multicomponente: Incidente que implica varios incidentes mencionados anteriormente.

- ✓ Otros Incidente: Incidente que no se puede clasificar en algunas de las categorías mencionadas anteriormente, por lo que la organización debe contemplar la necesidad de crear otra categoría que permita clasificarlo.

Los incidentes de seguridad se deben evaluar de acuerdo a su nivel de impacto de acuerdo al análisis de riesgos y a la clasificación de activos de información elaborado por la entidad y tener en cuenta que el evento reportado realmente sea un incidente que afecte la triada de la información (Confidencialidad, Disponibilidad e Integridad).

7.2.1 Niveles de severidad

- ✓ Alto Impacto: El incidente afecta activos de información con un impacto catastrófico afectando objetivos misionales de la organización.

- ✓ Medio Impacto: El incidente afecta activos de información con un impacto moderado influyendo en objetivos de procesos determinados.

- ✓ Bajo Impacto: El incidente afecta activos de información con un impacto menor que no influye en ningún objetivo de la empresa. Este tipo de incidentes deben ser monitoreados con el fin de verificar que el nivel de severidad de los incidentes no cambie.

7.3 Medidas para iniciar un procedimiento de evidencia digital

- ✓ De acuerdo a la “Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información”, verificar si el incidente realmente se presentó.
- ✓ Verificar si es procedente realizar el procedimiento de evidencia digital de acuerdo al incidente evidenciado.
- ✓ Minimizar la pérdida o alteración de la información.
- ✓ Realizar el control de las operaciones por medio de bitácoras que almacenen fechas y horas de su ejecución.
- ✓ Analizar los datos recolectados.
- ✓ Realizar reporte de hallazgos.

Figura 6. Diagrama del proceso de evidencia digital.

Fuente: MinTic https://www.mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf

Una vez se identifica que el evento reportado se clasifica como incidente de seguridad de la información se da inicio a la primera Fase.

7.4 Fases para llevar a cabo un proceso de evidencia digital

7.4.1 Fase 1. Alistamiento de la Escena

Restringir al acceso al lugar donde se originó o produjo el incidente con el fin de evitar alteraciones o sea contaminada la evidencia que posteriormente servirá para realizar la investigación respectiva.

El alistamiento de la escena puede ser realizado por una autoridad competente, pero con el fin de evitar una posible contaminación o alteración de la misma, puede ser realizada por un profesional del área de la seguridad informática o forense quien se encuentre en la capacidad de realizar una descripción detallada de los procedimientos llevados a cabo para aislar la escena y capturar evidencia en primera instancia.

A continuación, se describen procedimientos generales para llevar a cabo el alistamiento de la escena:

- ✓ Tomar fotografía del equipo o lugar del incidente antes de establecer algún tipo de contacto físico.
- ✓ Marcar un perímetro de seguridad con el fin de evitar el ingreso al sitio.
- ✓ No apagar el equipo en caso que se encuentre encendido.
- ✓ Sellar puertos USB y demás accesos (CD/DVD), entre otros para bloquear cualquier tipo de alteración.
- ✓ Tomar fotografías de ventanas abiertas, ya sean de programas, carpetas, archivos donde se observe hora y fecha.
- ✓ Si el equipo de cómputo se encuentra encendido asegurarse que mantenga la corriente eléctrica continua y evitar se apague.

- ✓ En lo posible capturar información volátil del equipo antes que este se apague pero haciendo uso de herramientas forenses necesarias.

- ✓ En caso de que el equipo se encuentre apagado no proceder a su encendido con el fin de evitar pérdida o alteración de datos.

- ✓ Contar con elementos necesarios para la recolección de información como dispositivos para backups, medios formateados y/o estériles, cámaras digitales, cinta y bolsas para evidencia, etiquetas, papel de burbuja, bolsas antiestáticas, cajas de cartón ,etc.

7.4.1.1 Cadena de Custodia

La cadena de custodia garantiza que las evidencias encontradas en el lugar de los hechos son realmente las que se están presentando ante el tribunal penal o comité disciplinario, evitando que la evidencia sea rechazada. Como mínimo una cadena de custodia debe presentar:

- ✓ Hoja de ruta: Datos principales sobre la descripción de las evidencias como fechas, horas, custodios, identificaciones, cargos y firmas de quien recibe y quien entrega.

- ✓ Recibos de cada custodio: En los cuales se encuentran datos similares a la hoja de ruta.

- ✓ Etiquetas o rótulos: Los que se usaron para marcar cada evidencia (sobres, cajas, bolsas).

- ✓ Entradas y Salidas: Libros o sistemas de información que son llevados en laboratorios de análisis, despechos fiscales e investigadores.

7.4.2 Fase 2. Identificación de fuentes de información

En el proceso de adquisición de información es muy importante identificar aquellas fuentes potenciales de las cuales será posible extraer datos con el fin de contar con el soporte de evidencia digital.

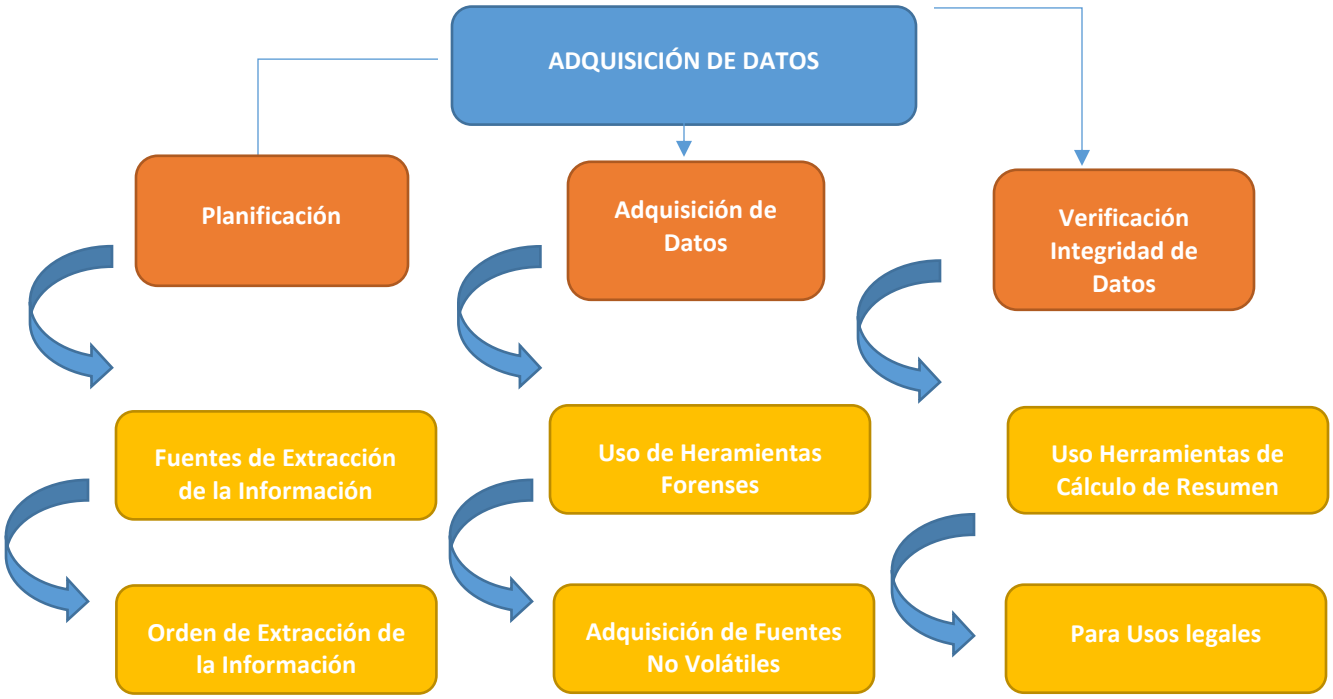
Las fuentes más usuales para hallar información son las siguientes:

- ✓ Computadores (ya sea de escritorio o portátiles).
- ✓ Servidores.
- ✓ Nube o almacenamiento en red.
- ✓ Dispositivos internos o externos como Discos duros, memorias USB, Firewire, CD/DVD, Discos ópticos y magnéticos, Discos duros extraíbles, Memorias SD y MicroSD, entre otros.
- ✓ Equipos celulares, Cámaras digitales, Grabadoras de Video y Audio.
- ✓ En cuanto a otras fuentes de información a nivel de seguridad informática se encuentran los registros de Logs tanto de: Dispositivos de seguridad como IDS, Firwalls, Plataformas antispam, Proxy, switches o routers, de proveedores de servicio, estos últimos solo es posible obtenerlos con una orden judicial.

7.4.2.1 Adquisición de Datos

El proceso de Adquisición de Datos debe ser realizado bajo un estricto orden y planificación previa, toda vez que si esta será utilizada para fines legales es clave implementar la cadena de custodia adecuadamente.

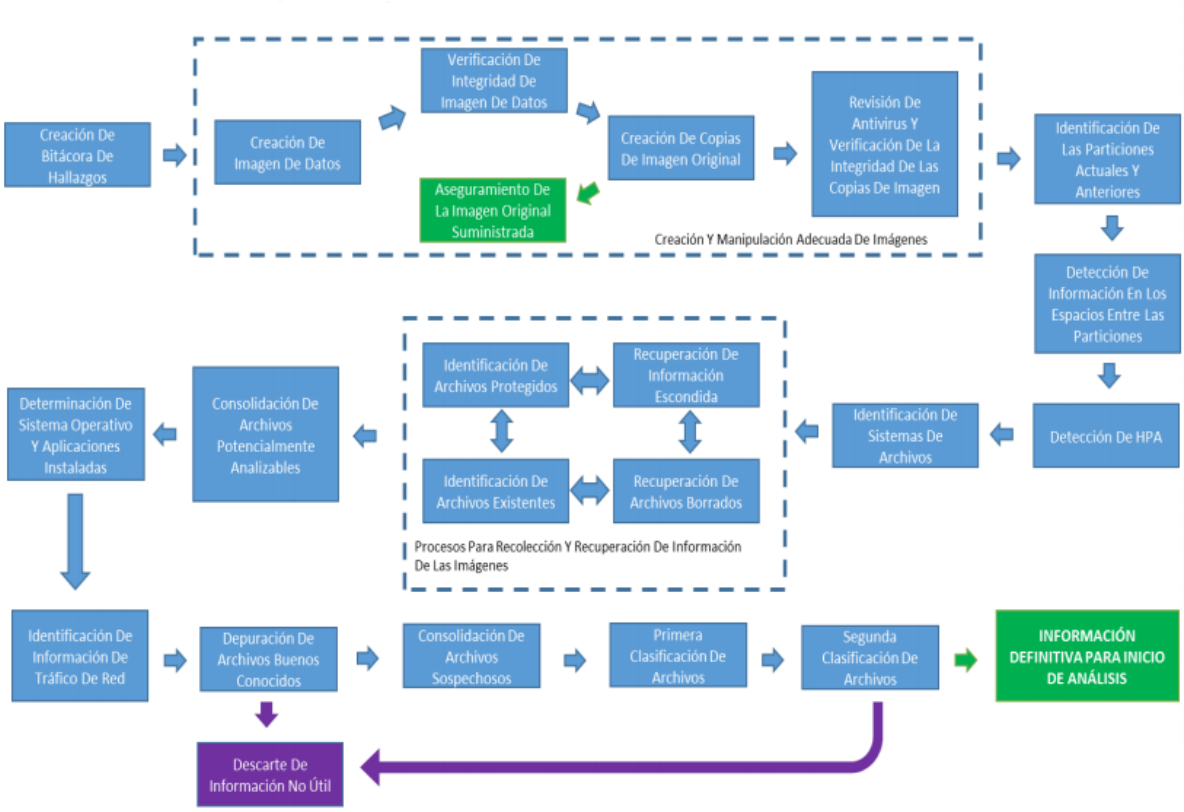
Figura 7. Adquisición de Datos



Fuente: MinTic https://www.mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf

7.4.3 Fase 3. Recolección y examinación de información

Figura 8. Diagrama de examinación y recolección de Información



Fuente: MinTic https://www.mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf

7.4.4 Fase 4. Análisis de la información

En esta fase se analizan aquellos eventos que fueron extraídos de las fuentes de información (fotografías logs, documentos, videos, entre otros.) y que se consideran importantes para su posterior estudio y lograr llegar a una conclusión.

Las siguientes etapas deber ser ejecutadas dentro de esta fase:

- ✓ Análisis de la Información Prioritaria

  Discriminar archivos prioritarios de acuerdo a su relevancia en el caso y el criterio investigador.

- ✓ Generación del Listado de archivos comprometidos en el caso

El investigador determinará cuáles archivos serán empleados como evidencia a presentar en informe final o en el proceso judicial

- ✓ Obtención de la línea de tiempo de la evidencia

Los hechos deben ser reconstruidos y esto se debe hacer a partir de los atributos de fecha y hora de los archivos con el fin de crear una correlación lógica que integre positivamente la evidencia.

- ✓ Generación de Informe final

Informe de hallazgos donde se describen detalladamente los hechos importantes ocurridos y relata la manera como se encontraron, tomando como base la documentación continúa de la aplicación metodológica.

7.4.5 Fase 5. Reporte

El reporte expone toda la información y evidencia obtenida en la fase de análisis y debe contener la siguiente información.

Figura 9. Mapa mental Fase de Reporte

Fuente: MinTic https://www.mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf

7.5 Realidades de la Ciberdelincuencia en Colombia

El 15 de febrero de 2018 la revista Semana publica el artículo “se disparó el delito” donde se menciona el crecimiento dramático del hurto, delitos informáticos y sexuales durante el año.

De acuerdo al censo semanal de la Fiscalía, el hurto abarca una tercera parte de los delitos cometidos, le siguen los delitos informáticos, donde los más investigados son el phishing o el robo de datos por medio de páginas web, siendo este tipo de delitos los que más se articulan internacionalmente, afirma Wilson Pardo, subdirector de la DIJIN, además que el comportamiento de las personas en las redes permite a los delincuentes llevar a cabo sus objetivos criminales.

Pardo agrega, que entre los años 2016 a 2018 se han recibido 31.248 denuncias de tipo abuso a un sistema informático, transferencia de datos ilegalmente, entre otros; pero que a pesar de las diversas herramientas para actuar y denunciar las personas siguen cayendo y replicando comportamientos inseguros en la red.

En el artículo publicado por la revista dinero el día 06 de Enero de 2019 denominado “Guía de ciberseguridad para el 2019”, se menciona que a pesar de conocer las vulnerabilidades que implica estar conectados a la red, el 87% de las organizaciones más grandes del mundo operan con niveles limitados de ciberseguridad y el 77% implementa medidas básicas de ciberseguridad y buscan avanzar en la implementación de técnicas avanzadas como son, la inteligencia artificial, automatización robótica de procesos, analítica de datos, entre otros.

Lo anterior resulta alarmante y contradictorio, dadas las lecciones que el mundo ha dejado a nivel de vulnerabilidades corporativas; pero aún existe una resistencia de las directivas para invertir mayores recursos en la implementación de altos niveles de seguridad que minimice el impacto que puedan causar los miles de ataques que diariamente son lanzados por los ciberdelincuentes y que son automatizados y perfeccionados con el fin de encontrar brechas de seguridad pero a su vez podemos identificar que un 77% de las grandes organizaciones buscan crecer e innovar en el tema de la ciberseguridad.

7.5.1 Custodia de Evidencia- Caso “Raúl Reyes”

El 01 de marzo del 2008 el Ejército Colombiano llevó a cabo la “Operación Fénix”, en la cual fue abatido en territorio ecuatoriano, Edgar Devia Silva, más conocido por su alias “Raúl Reyes”, comandante de las FARC.

En el desarrollo de la operación se encontraron computadores y dispositivos de almacenamiento, los cuales fueron trasladados a territorio colombiano por el Comando de Operaciones Especiales “COPES”. Teniendo en cuenta que la evidencia se encontraba en el extranjero, se debía llevar a cabo el proceso de custodia por medio de los protocolos exigidos por la legislación colombiana y por los convenios internacionales en materia probatoria, como lo son el Código del Procedimiento Penal Colombiano y el Convenio de Cooperación Judicial y asistencia mutua en Materia Penal, celebrado entre Colombia y Ecuador y ratificado por el Congreso de la República mediante la Ley 519 de 04 de Agosto de 1999.

La Sala Penal de la Corte Suprema de Justicia reiteró el fallo mediante el cual se declaran como inválidas las pruebas tomadas de los medios electrónicos hallados en la Operación Fénix debido a que no se llevó a cabo el “debido proceso” para recuperar los archivos, rompiendo la cadena de custodia e incumpliendo el peritaje forense, omitiendo el protocolo legal que exige una operación internacional.

En los computadores hallados se encontró el nombre del político sindicalista Wilson Alfonso Borja Díaz, de quién la Sala Penal de la Corte Suprema de Justicia confirmó el archivo del proceso y del cual a pesar de no ser posible iniciar un proceso penal debido a la invalidez de las pruebas, fue investigado por sus supuestos nexos con el grupo guerrillero.

Al igual que el caso mencionado anteriormente, se generaron otros comentarios y acusaciones en contra de altos funcionarios del Gobierno, del Ejército, de la Policía Nacional y hasta del entonces presidente de la República Alvaro Úribe Vélez, basándose en documentos de evidencia digital recuperada de los dispositivos hallados, pero finalmente solo se logró comprobar el desconocimiento legal y normativo frente a la correcta recolección de evidencia digital por parte del Gobierno Nacional y de la fuerza pública.

Según el auto 29877 de 18 de Mayo de 2011 proferido por la Corte Suprema de Justicia donde uno de los puntos se refiere al carácter ilegal de la prueba. *“Conforme lo ordena la constitución política las leyes y los tratados internacionales, ninguna*

autoridad colombiana tiene competencia o está facultada para practicar en el extranjero inspecciones y recoger elementos materiales de conocimiento, por fuera de los mecanismos de la cooperación internacional y la asistencia judicial de las autoridades del estado concernido, la producción o práctica de pruebas en el exterior también atienden a un debido proceso no se pueden recoger de manera informal, de facto, sino siguiendo un método legal la prueba recogida de otro modo es ilegal y no puede ser admitida en el mundo jurídico para sustentar ningún propósito procesal."

Frente al caso "Raul Reyes" es posible señalar que el resultado de los que sería una operación exitosa realmente no tuvo los efectos esperados, se generaron expectativas a nivel de país frente al impacto que tendría la evidencia digital hallada, pero finalmente el desconocimiento de las autoridades frente a los procedimientos y el interés de mostrar resultados rápidamente dieron pie a que se invalidaran pruebas que pudieron ser de carácter punitivo y claves para comprobar nexos de altos funcionarios del estado con el grupo de las FARC.

CAPITULO III

CONSIDERAR LA IMPORTANCIA DE LA SENSIBILIZACIÓN EN EL USO DE LAS TECNOLOGÍAS PARTIENDO DEL PRINCIPIO DE PREVENCIÓN DE POSIBLES SITUACIONES.

En este capítulo se enfoca en la prevención de posibles situaciones que se pueden materializar desde un enfoque particular y también empresarial, teniendo en cuenta que cuando un individuo decide ser preventivo al momento de usar las tecnologías de la información a nivel personal, igualmente existe una alta probabilidad de que replique este tipo de comportamiento cuando se encuentra en su lugar de trabajo.

Aquellas organizaciones ya sean públicas o privadas que implementan Sistemas de Gestión de la Seguridad de la Información por lo general promueven en los empleados prácticas de prevención contra incidentes de seguridad de la información, sensibilizando frente a los tipos de amenazas que se generan a medida que el uso de las tecnologías continúa su auge.

8.1 Uso de Sistemas de Gestión de Seguridad de la Información (SGSI).

Un Sistema de Gestión de Seguridad de la Información (SGSI) debe encontrarse alineado con las buenas prácticas de seguridad, además con los cambios técnicos que da la norma ISO/IEC 27001:2013, la cual es la norma internacional que describe la manera como se debe gestionar la seguridad de la información en una organización del sector privado o público de cualquier dimensión, permitiendo su certificación, confirmando que la empresa cumple con la norma ISO 27002.

8.1.1 Beneficios certificación ISO 27002:2013

Cumplimiento de Requerimientos Legales: Frecuentemente se crean y modifican leyes, normativas, requerimientos relacionados con seguridad de la información que de manera inherente al implementar adecuadamente la metodología de la norma se daría cumplimiento a estos requisitos legales.

- ✓ Ventaja comercial: Los clientes desean que su información se encuentre segura con una organización que cuenta con la certificación ISO 27001 lo cual puede generar una ventaja frente a la competencia que tal vez no cuenten con dicha certificación. En el sector público se adquiere confianza por parte de los usuarios, ciudadanos.

- ✓ Menores costos: Cuando se presentan incidentes de seguridad ya sean de alto o bajo impacto, esto acarrea una serie de gastos para la organización, motivo por el cual la implementación de la norma ISO 27001 representa una inversión dado que su metodología previene y reduce la presentación de los incidentes de seguridad.

- ✓ Organización de la empresa: Conocimiento y claridad en las funciones que debe desempeñar cada empleado, reduciendo tiempo perdido por el desconocimiento los procesos que se desarrollan y por parte de los trabajadores frente a las labores que deben desempeñar. Para empresas públicas se cumpliría con la obligación de ajustar el sistema al sector que maneja.

Si bien el beneficio más visible para una organización es dar a conocer su certificación en la norma ISO 27001 a nivel interno se desglosan una cantidad de ventajas que finalmente se verán reflejadas exteriormente, beneficiando a proveedores, clientes, entre otros.

8.2 Modelo de seguridad y privacidad de la información – Gobierno en línea- Ministerio de las TIC.

8.2.1 Antecedentes

El decreto 1078 de 2015 expide un decreto único reglamentario frente al sector de las tecnologías de la información y las comunicaciones. El título 9 de este decreto señala “POLÍTICAS Y LINEAMIENTOS DE TECNOLOGÍAS DE LA INFORMACIÓN, CAPITULO 1, Estrategia de Gobierno en Línea, en la SECCIÓN 2, COMPONENTES, INSTRUMENTOS Y RESPONSABLES, se define el componente de seguridad y privacidad de la información, como parte integral de la estrategia Gobierno en Línea, y es de **obligatorio cumplimiento para las entidades del estado** como lo establece en la sección 3, MEDICIÓN, MONITOREO Y PLAZOS.

Se resalta la frase “obligatorio cumplimiento para las entidades del estado”, lo cual implica que especialmente aquellos profesionales que desempeñan labores en áreas relacionadas con la seguridad informática deben como mínimo conocer el Modelo Seguridad y Privacidad de la Información (MSPI), elaborado por el Ministerio de las TIC, donde se recopilan las mejores prácticas, nacionales e internacionales, que brindan una línea y se establecen los requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo.

La guía permite actualizaciones con el fin de estar alineada con las normas internacionales ISO 27001, Cobit, ITIL, Marco de Referencia Arquitectura TI, así mismo frente a las recomendaciones de mejores prácticas que realicen organizaciones como el Convenio de Budapest (ciberdelincuencia) y la Organización para la Cooperación y el Desarrollo Económico (OCDE).

En los últimos años, la implementación de la Guía de Seguridad y Privacidad de la Información por parte de entidades del país ha contribuido al fortalecimiento de la seguridad de la información, en busca de garantizar su confidencialidad, disponibilidad e integridad. El modelo se encuentra alineado con la legislación actual colombiana, incluyendo en su nueva actualización el nuevo marco normativo relacionado con protección de datos personales, transparencia y acceso a la información pública, entre otras.

8.2.2 Fases de Aplicación- Modelo de Seguridad y Privacidad de la Información.

El MSPI se divide en 5 fases con varios niveles de madurez con la finalidad de facilitar el entendimiento de su aplicación por parte de las entidades y sea posible una adecuada gestión de sus activos, contribuyendo con el cumplimiento de sus objetivos misionales.

:

8.2.2.1 Modelo de Operación

Las cinco fases del modelo establecen objetivos, metas y herramientas que fueron creadas con el objetivo de que el sistema de gestión de seguridad y privacidad de

la información sea sostenible. A continuación, se ilustran las fases que presenta el modelo:

- ✓ Fase 1: Etapa previa a la implementación
- ✓ Fase 2: Planificación
- ✓ Fase 3: Implementación
- ✓ Fase 4: Gestión
- ✓ Fase 5: Mejoramiento continuo

Figura 10. Marco de Seguridad y Privacidad de la Información

Fuente: MinTic http://estrategia.gobiernoenlinea.gov.co/623/articles-8258_recurso_1.pdf.

- ✓ **Fase 1: Etapa previa a la implementación**

En esta fase previa la entidad debe determinar los siguientes elementos:

- ✓ Estado en que se encuentra frente a la gestión de seguridad y privacidad de la información.
- ✓ Establecer un nivel de madurez de seguridad y privacidad de la información.
- ✓ Levantamiento de la información para realizar pruebas de efectividad con el fin de medir los controles existentes.

Figura 11: Etapas previas a la implementación

Fuente: MinTic http://estrategia.gobiernoenlinea.gov.co/623/articles-8258_recurso_1.pdf.

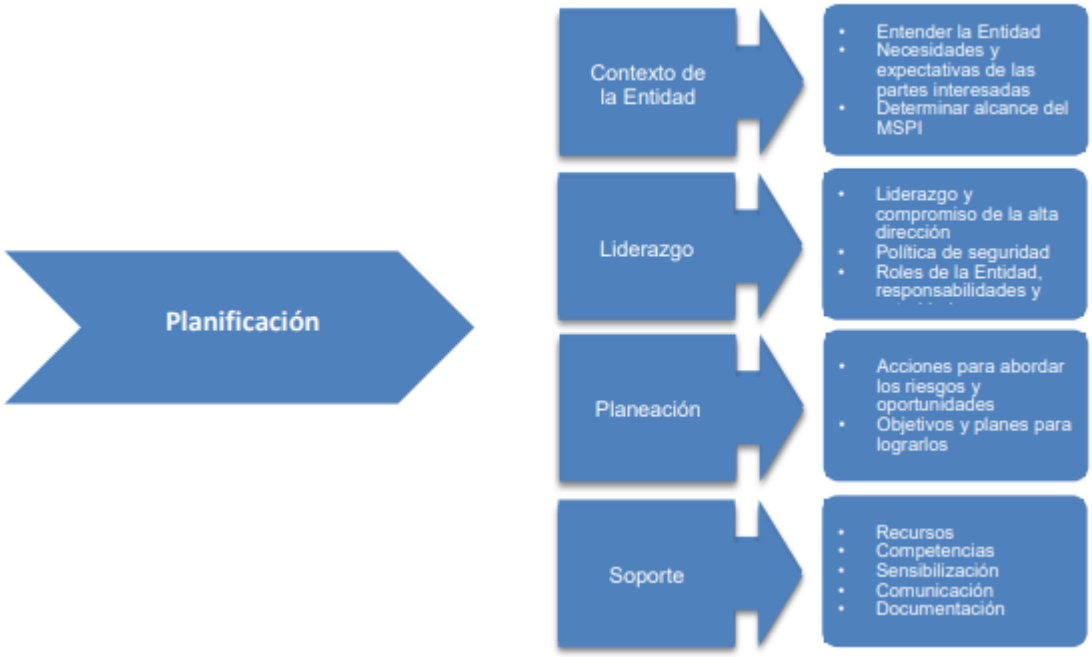
- ✓ **Fase 2: Planificación**

Un plan de Seguridad y Privacidad de la Información alineado con los objetivos misionales de la entidad es el propósito principal de esta fase.

Esta fase busca el cumplimiento de una serie de metas, resultados e instrumentos.

A continuación, se ilustran los elementos que contiene la fase de planificación:

Figura 12. Fase de planificación



Fuente: MinTic http://estrategia.gobiernoenlinea.gov.co/623/articles-8258_recurso_1.pdf.

Las metas que la fase de planificación establece se deben alcanzar frente a la seguridad y privacidad de la información son:

- ✓ Objetivos y alcance del plan de seguridad y privacidad de la información

Cumplimiento de la triada de la información (Confidencialidad, disponibilidad e integridad) con el fin de garantizar el cumplimiento de los objetivos misionales de la entidad.

- ✓ Políticas de seguridad y privacidad de la información

Declaración de compromiso de la alta gerencia frente a la implementación del MSPI.

- ✓ Procesos y procedimientos definidos

En cada área de la entidad deben ser implementados unos procedimientos mínimos relacionados con controles de seguridad y privacidad de la información.

- ✓ Asignación de recurso humano roles y responsabilidades.

La implementación del MSPI implica la necesidad de un recurso humano disponible para las gestiones que requiera el modelo, así mismo es muy importante definir roles y responsabilidades claras frente al proceso.

- ✓ Integración del MSPI con el sistema de gestión documental

- ✓ Identificación y descripción de activos de información que contengan datos personales.

Es necesario realizar dicha descripción con el fin de determinar el tratamiento de acuerdo a la valoración realizada en el inventario.

- ✓ Acciones de tratamiento de riesgos y oportunidades de seguridad de la información

Es importante utilizar una metodología de gestión del riesgo enfocada a procesos.

- ✓ Aprobación de resultados por parte de la alta dirección

- ✓ **Fase 3: Implementación**

Esta fase permite a la organización llevar cabo los resultados obtenidos en las fases anteriores y teniendo en cuenta sus necesidades se procede a elaborar el plan de implementación, el plan de tratamiento de riesgos y el plan operacional. A continuación, se ilustran las fases de la implementación:

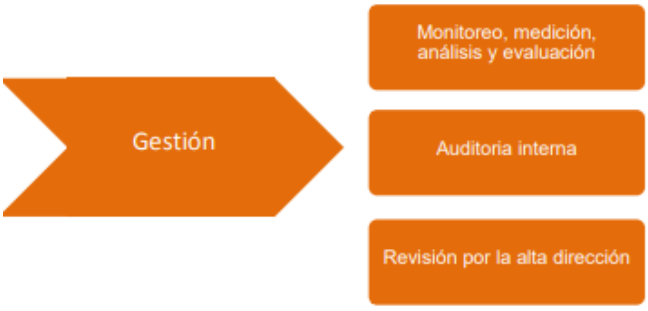
Figura 13. Fase de implementación

Fuente: MinTic http://estrategia.gobiernoenlinea.gov.co/623/articles-8258_recurso_1.pdf.

- ✓ **Fase 4: Evaluación de desempeño**

La fase de Evaluación de desempeño entrega los procesos de seguimiento y monitoreo tomando como base los resultados arrojados por los indicadores de seguridad de la información que fueron propuestos para medir la eficacia y efectividad de los controles implementados.

Figura 9. Fase de Evaluación de desempeño



Fuente: MinTic http://estrategia.gobiernoenlinea.gov.co/623/articles-8258_recurso_1.pdf.

Para la definición de la fase de evaluación de desempeño se deben considerar los siguientes elementos:

- ✓ Actividades dentro del Modelo de seguridad y privacidad de la información que deberán ser monitoreadas y evaluadas.
- ✓ Acciones necesarias para el seguimiento y evaluación.
- ✓ Responsable de las acciones de seguimiento y evaluación.
- ✓ Oportunidad y periodicidad de las acciones de seguimiento y evaluación.
- ✓ Metodología de seguimiento y evaluación.
- ✓ Recursos requeridos para el plan de seguimiento.

Los resultados del Plan de Seguridad de la Información deben ser difundidos a los interesados en la organización.

- ✓ **Fase 5: Mejora continua**

La última fase del modelo tiene como objetivo la consolidación de los resultados arrojados por la fase de evaluación de desempeño con el fin de diseñar el plan de mejoramiento continuo de seguridad de la información para posteriormente desarrollar el plan de implementación de las acciones correctivas que fueron encontradas.

Figura 15. Fase de mejoramiento continuo

Fuente: MinTic http://estrategia.gobiernoenlinea.gov.co/623/articles-8258_recurso_1.pdf.

En esta fase la organización debe definir y ejecutar el plan de mejora continua teniendo en cuenta resultados de la fase de evaluación de desempeño.

8.3 Uso del Internet, Sensibilización desde la Primera Infancia.

Como se menciona al inicio del este capítulo, una vez las personas se concientizan y deciden hacer buen uso de las tecnologías de la información a nivel personal, igualmente replicarán dicho comportamiento a nivel laboral; por lo tanto es indispensable que desde la niñez se promueva tanto a nivel familiar como educativo el buen uso de los recursos informáticos, especialmente cuando dichos recursos informáticos permiten a niños y jóvenes estar interconectados, acceder a toda la información que les puede interesar, conectarse con otras personas en cualquier parte del mundo y un sinfín más de posibilidades.

La red Papaz es una entidad fundada en el año 2003, cuyo objetivo principal es abogar por los derechos de los niños, niñas y adolescentes en el país, además fortalecer las capacidades de los adultos y actores sociales con el fin de garantizar su efectivo cumplimiento. La red Papaz promueve el uso sano, seguro y constructivo del Internet, dando a conocer diez recomendaciones que las familias deben tener en cuenta para hacer uso responsable de la tecnología:

- ✓ Generación de espacios de diálogo.

Dada la brecha existente entre padres que experimentaron el uso de las tecnologías cuando ya eran adultos, con respecto a sus hijos que nacieron sumergidos en este mundo cibernético, y cuyo término “nativos digitales”, se refiere al dominio de la tecnología que los hijos han adquirido desde su primera infancia; es necesario entre padres e hijos fortalecer vínculos, compartir sus experiencias adquiridas en el mundo informático con el fin de evitar el aislamiento entre ambos.

- ✓ Comunicar situaciones de vulnerabilidad.

Dar a conocer cualquier situación negativa, ya sea a la familia, adultos de confianza o denunciar ante las autoridades, las cuales cuentan con diversos canales de atención para encargarse de situaciones como pornografía infantil, ciberacoso, chantaje, entre otras.

- ✓ Pensar antes de publicar.

Prudencia al momento de publicar información personal, familiar, financiera, económica, laboral, la cual pueda ser utilizada en contra del usuario.

- ✓ Ser respetuosos.

Diversidad de pensamientos, opiniones, pueden llevar a caer en ambientes violentos, ya sea por comentarios o simplemente un “me gusta”, no caer en el juego de responder comentarios negativos o promoverlos.

- ✓ La regla 3, 6, 9, 12.

Teniendo en cuenta una investigación realizada en Francia, la cual fue avalada por la asociación de Pediatría se recomienda:

Niños de entre 0 y 3 años: No tener contacto con pantallas dado que es poco lo que aportan a su desarrollo.

Entre 3 y 6 años: No tener acceso a videojuegos dado que a estas edades resultan ser altamente adictivos.

Entre 6 y 9 años: Pueden usar computadores y otros dispositivos, pero sin conexión a internet.

A partir de los 12 años: Pueden usar computadores y otros dispositivos con conexión a internet pero bajo la supervisión permanente de un adulto responsable.

- ✓ Considerar las normas básicas del internet

No todo lo que muestra el internet es cierto. Cualquier información publicada será de dominio público y pueden permanecer para siempre en miles de servidores, así se piense que esta fue dada de baja.

- ✓ Educar a partir del ejemplo.

Los padres o acudientes son los encargados de enseñar a través del ejemplo, además de establecer normas claras frente al uso de dispositivos tecnológicos en ciertos lugares, horarios y demás.

- ✓ Enseñar en vez de prohibir.

Explicar de manera clara a niños y jóvenes el por qué no deben acceder a ciertas páginas, descargar aplicaciones, publicar información, establecer contacto con otros usuarios, mas no prohibir sin brindar claridad frente a dichas acciones.

- ✓ Hay otras formas de entrenamiento.

La familia debe disfrutar de otros tipos de entretenimiento que no involucren el uso del internet.

- ✓ Aprovechar espacios de capacitación.

Dado que cada día se generan nuevas amenazas en el uso de las tecnologías de la información, las familias deben conocer y estar al tanto de este tipo de elementos que pueden vulnerar a sus hijos, aprender cómo prevenir situaciones es lo más importante a la hora de proteger a los niños y jóvenes.

9. CONCLUSIONES

Las conclusiones de esta monografía se obtuvieron luego de documentar cada uno de los objetivos específicos, los cuales conllevaron principalmente a identificar la importancia de la legislación vigente en seguridad informática en Colombia y las consideraciones necesarias a la hora de denunciar un delito informático.

A continuación, se puntualizan las conclusiones específicas que constituyen los resultados de la monografía:

- ✓ Colombia requiere crecer en temas de legislación informática, contar con especialistas en área de la seguridad informática que trabajen articuladamente con profesionales del ámbito jurídico siendo posible tipificar aquellos delitos informáticos correctamente.

- ✓ Fortalecimiento del sistema judicial en el país, enfocándose desde la prevención de situaciones. Gran cantidad de denuncias relacionadas con delitos informáticos son entabladas por ciudadanos diariamente a la Fiscalía, organismo encargado de brindar a la comunidad una cumplida y eficaz administración de la justicia; pero que no cuenta con la cantidad suficiente de profesionales especializados en el área de la informática que gestionen los casos con la oportunidad requerida.

- ✓ Implementación de la estrategia Gobierno en Línea en todos los niveles. La estrategia Gobierno en Línea debe ser conocida y estudiada por los profesionales en el área de la seguridad informática, dado que plantea un modelo aplicable a entidades del estado, organizaciones privadas de cualquier tamaño, frente a aquellas acciones tendientes a proteger la información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.

- ✓ Mayor compromiso del estado con el uso del internet. La estrategia Gobierno en Línea promueve el uso y apropiación de las Tecnologías de la Información en el territorio nacional; pero esto debe ir de la mano con la sensibilización de la población frente a su uso; establecer estrategias que permitan que tanto niños, adolescentes y adultos adopten medidas de protección frente a posibles situaciones.

BIBLIOGRAFIA

1. Cisneros, E. M. (2012). Cómo elaborar trabajos de grado [en línea] 2. ed.). Bogotá, CO: Ecoe Ediciones. Disponible en Internet: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=10626100&p00=icontec+ntc+1486

2. Congreso de Colombia. Ley 1273 de 2009 [en línea] Bogotá. Disponible en Internet https://www.mintic.gov.co/portal/604/w3-article-3705.html

3. 2018. Colombia el sexto país con más ciberataques en 2017 [en línea] Envigado, Antioquia. Disponible en internet: http://www.elcolombiano.com/colombia/ciberataques-en-colombia-sexto-pais-mas-vulnerable-en-la-region-AB8535174

4. Manjarrés, I & Jiménez, F. (2012). Caracterización de los delitos informáticos en Colombia [en línea]. Barranquilla, Medellín. Disponible en internet: https://www.coruniamericana.edu.co/publicaciones/ojs/index.php/pensamientoamericano/article/viewFile/126/149

5. Agencia AFP. El hackeo de autos y los peligros de la Internet de las cosas [en línea]. Disponible en Internet: http://www.elcomercio.com/guaifai/hackeo-autos-peligros-internet-cosas.html

6. Gutiérrez, de Mesa, José Antonio, and Arévalo, Carmen Pagés. Planificación y gestión de proyectos informáticos, Servicio de Publicaciones. Universidad de Alcalá, 2008. ProQuest Ebook Central, Disponible en Internet: http://bibliotecavirtual.unad.edu.co:2460/lib/unadsp/detail.action?docID=3176931.

7. Fundación Wikimedia. Definición WhatsApp [en línea]. Disponible en Internet: https://es.wikipedia.org/wiki/WhatsApp

8. Roa, Buendía, José Fabián. Seguridad informática, [en línea] McGraw-Hill España, 2013. ProQuest Ebook Central, Disponible en Internet: http://bibliotecavirtual.unad.edu.co:2460/lib/unadsp/detail.action?docID=3211239.

9. Martínez, La Patria. Colombia, el primer país que penaliza los delitos informáticos [en línea]. Manizales. 2012. Disponible en Internet: http://www.lapatria.com/tecnologia/colombia-el-primer-pais-que-penaliza-los-delitos-informaticos-1980

10. Ramírez, Aguilera. Los Delitos Informáticos. Tratamiento Internacional [en línea] 2009. Disponible en Internet: http://www.eumed.net/rev/cccss/04/rbar2.htm

11. Ojeda, Rincón, Arias, Daza. Delitos informáticos y entorno jurídico vigente en Colombia [en línea]. 2010. Bogotá. Disponible en Internet: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003

12. Pérez. ¿En Colombia se investigan los delitos informáticos? [en línea]. 2013. Disponible en Internet: https://colombiadigital.net/actualidad/articulos-informativos/item/4810-en-colombia-se-investigan-los-delitos-informaticos.html

13. Téllez. IIJUNAM. Derecho Informático [en línea]. 2012. Disponible en Internet: http://www.youtube.com/watch?v=ubi5DSu06ro

14. Legislación Informática. Disponible en https://derechoinformtico.wordpress.com/2015/07/22/legislacion-informatica/

15. López. Las nuevas fronteras de la seguridad informática [en línea]. 2015. Disponible en Internet: http://www.expansion.com/economia-digital/innovacion/2017/03/11/58c159f9268e3e12778b4625.html

16. Las mejores frases de seguridad informática [en línea]. 2017. Disponible. https://protegermipc.net/2017/04/04/las-mejores-frases-sobre-seguridad-informatica/

17. Ley 1273 de 2009 [en línea]. 2009. Disponible. http://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

18. Ley Estatutaria 1581 de 2012. Disponible en http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

19. Ley 1341 de 2009 Nivel Nacional. Disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36913

20. Guía # 13. Evidencia Digital. Seguridad y Privacidad de la Información, Disponible en https://www.mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf

21. Guía # 25. Gestión y Clasificación de Incidentes de Seguridad de la Información, Seguridad y Privacidad de la Información. https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

22. ¿Definición norma ISO 27001? https://advisera.com/27001academy/es/que-es-iso-27001/

23. Sistemas de Gestión de la Seguridad de la Información (SGSI. https://www.mintic.gov.co/gestionti/615/w3-article-5482.html

24. El decálogo del buen uso de internet, según los adolescentes. Disponible en https://www.eltiempo.com/archivo/documento/CMS-13989636

25. ¿Quiénes somos?. Disponible en: https://www.fiscalia.gov.co/colombia/la-entidad/quienes-somos/

26. Documento ¿Qué es Red Papáz? Disponible en https://www.redpapaz.org/category/informacion-red-papaz/documento-de-informacion-basica/

27. Diez recomendaciones para usar Internet de forma segura en el hogar. Disponible en: https://www.redpapaz.org/aprendiendoaserpapaz/index.php?option=com_k2&view=item&id=503:10-recomendaciones-para-usar-internet-de-forma-segura-en-el-hogar&Itemid=147

28. La verdad judicial a 4 años del escándalo del 'hacker' Sepúlveda. Disponible en https://www.eltiempo.com/justicia/delitos/hacker-andres-sepulveda-proceso-cuatro-anos-despues-219446

29. 10 Años de Prisión por Delitos Informáticos para Andrés Sepúlveda. Disponible en http://derechoinformatico.co/10-anos-de-prision-a-andres-sepulveda-por-delitos-informaticos/

30. Guía de ciberseguridad para el 2019 Disponible en https://www.dinero.com/tecnologia/articulo/ciberseguridad-en-el-2019-en-colombia/265858

31. Colombia se rajó por falta de civismo y fraude en la red Disponible en https://www.publimetro.co/co/bogota/2018/02/15/delitos-informaticos-que-mas-se-cometen-en-colombia.html

32. Se disparó el delito. Disponible en https://www.semana.com/nacion/articulo/cifras-de-cuantos-delitos-se-han-cometido-en-colombia-estadistica-del-dia/557161

33. AUTO 29877 DE 18 DE MAYO DE 2011. CORTE SUPREMA DE JUSTICIA. Disponible en:

http://legal.legis.com.co/document/index?obra=jurcol&document=jurcol_a47f3befffb700e4e0430a01015100e4

34. Corte explica fallo que declaró ilegales correos de PC de 'Raúl Reyes' Disponible en: https://www.eltiempo.com/archivo/documento/CMS-9451804

35. PC de 'Reyes' no sirve para construir un proceso, pero sí como base de investigación: Corte. Disponible en: https://www.semana.com/nacion/articulo/pc-reyes-no-sirve-para-construir-proceso-pero-si-como-base-investigacion-corte/244119-3

36. Wilson Borja. Disponible en: https://es.wikipedia.org/wiki/Wilson_Borja

37. CaiVirtual. Amenazas del cibercrimen en Colombia. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

38. Datos abiertos de la Fiscalía General de la Nación. Disponible en: https://www.fiscalia.gov.co/colombia/gestion/estadisticas/