INFORMÁTICA FORENSE

Laura Herrera

EJE 2

Analicemos la situación

Fuente: Shutterstock/258980774

AREANDINA
Fundación Universitaria del Área Andina
MIEMBRO DE LA RED
ILUMNO

ÍNDICE

INTRODUCCIÓN

Nuestro trabajo de investigación forense ha iniciado. El desarrollo adecuado del eje epistemológico nos entregó las bases para conocer en detalle los conceptos, los procedimientos y los métodos, para acometer con éxito la tarea de realizar una investigación de carácter forense a un sistema de procesamiento automático de información.

Vamos por nuestra primera investigación. Este escenario reúne elementos que a diario podemos identificar en las noticias: en una localidad de la ciudad y luego de varias discusiones debido al carácter posesivo del compañero sentimental de la mujer, ella toma la decisión de separarse; para protegerse del acoso y presión de su expareja se traslada a otra localidad e inicia una nueva relación con un compañero de trabajo. Su expareja no se resigna a perderla e inicia una campaña de acoso a través de su correo electrónico, aprovechando que tiene algunas fotografías íntimas de ella, se las envía usando su correo electrónico y le pide regresar a su lado o hará públicas las fotos y alguna información adicional.

La mujer preocupada solicita la intervención de las autoridades, el investigador se encarga de iniciar el proceso, como primer paso le solicita a la afectada que abra su correo para revisar los mensajes que ha recibido dando apertura formal a la investigación. Pero, ¿acaso está olvidando algo? A partir de los contenidos y conceptos que ya se han desarrollado, ¿podemos inferir si la actuación del investigador es correcta?

Para una investigación forense exitosa debemos cumplir un conjunto de normas y técnicas que aseguren la recolección, adquisición, análisis y elaboración de los informes y en todos los pasos cumplir con la cadena de custodia. ¿Cumplir con estos requisitos es suficiente o se requiere algo más?

El correo electrónico de la afectada es un elemento propio de la órbita personal de los ciudadanos y por tanto se considera una extensión de su **intimidad**. Con base en esta premisa a pesar de contar con autorización de la "víctima" ¿puede el investigador revisarlo junto a ella? Existen aún demasiadas preguntas que debemos responder antes de acometer la tarea de iniciar y desarrollar la investigación. Así durante el desarrollo del eje sociocrítico abordaremos las tensiones que pueden existir producto de los derechos fundamentales en relación con las normas, códigos y legislación vigente.

Intimidad

Hace referencia a todo lo que corresponde a la esfera privada y particular de cada ser humano, y permanece dentro de sí, sin lugar a exposición pública.

Investigaciones que se pueden desarrollar con análisis forense digital

1. Investigación de hechos delictivos o criminales: la evidencia digital puede ser usada como prueba en investigaciones que implican el desarrollo de conductas criminales tipificadas en el código penal, como homicidios, trata de personas, fraude, estafa, contrabando, tráfico de sustancias ilícitas, tráfico de armas, pedofilia, entre otros.

2. Usos cotidianos en hogar y pequeña empresa (SOHO): cada día existen más herramientas que permiten desde recuperar un archivo borrado en una memoria USB, hasta la información contenida en un disco duro que se ha particionado o formateado.

3. Investigaciones relacionadas con el derecho civil: en procesos de divorcio, sucesiones, fraudes, casos de discriminación puede usarse la investigación digital forense para contribuir en el análisis de evidencia y su uso como prueba.

4. Investigaciones internas: al interior de las organizaciones pueden presentarse casos de robo de información, acceso sin autorización a información confidencial, intento de acceso a equipos no autorizados, que a pesar de no constituir conducta penal o delictiva puede comprometer la continuidad del negocio.

5. Investigaciones relacionadas con aseguradoras: las compañías de seguros luego de una reclamación por un siniestro adelantan una serie de averiguaciones para verificar que las condiciones establecidas en las pólizas se cumplan para hacer efectivas las coberturas. Así en un computador por ejemplo se puede encontrar información que puede ayudar para reducir una responsabilidad eventual.

6. Actividades legales de prevención: información depositada en conversaciones u ordenadores puede ser usada previa orden judicial para evitar que se cometa un delito.

Tipificado(a)

Término usado con más frecuencia en el derecho para agrupar conductas o elementos bajo una norma o tipo común.

Pedofilia

Hace referencia a cualquier tipo de acto de carácter sexual que se realice con un menor de edad, o en el que se emplea a menores de edad para causar placer, puede ser de forma directa o a través de videos, conversaciones o cualquier medio de difusión. (la definición de los menores de edad que se maneja para efectos del delito varía según la legislación de cada país, para Colombia menores de 14 años).

Sucesión

Termino relacionado con el derecho civil que hace referencia al proceso según el cual todos los bienes, obligaciones y derechos de un ciudadano se transfieren a una o varias personas luego de su muerte. Las personas que reciben la sucesión se definen según su grado de parentesco de acuerdo a la legislación de cada nación.

Fraude

Acción en la que una persona o grupo de personas engañan o se aprovechan de un error de otro u otros para alcanzar un beneficio de forma irregular u obtener lucro económico. Las modalidades de fraude se definen en la legislación de cada país.

Penal

Hace referencia a una conducta, entendida esta como cualquier comportamiento humano que se manifiesta de forma externa y produce un resultado, que en este caso contraviene una norma o vulnera un derecho de un individuo, comunidad u organización dando lugar a un castigo.

Siniestro

Evento accidental, fortuito o imprevisto en el que se causa un daño en bien propio o en el de un tercero. Entre los bienes no solo se habla de los materiales, también la vida, honra, dignidad, buen nombre son bienes definidos así por la legislación colombiana.

Póliza

Contrato suscrito entre un individuo u organización y una compañía de seguros a través del cual la aseguradora se compromete a cubrir, reponer o indemnizar al asegurado por las pérdidas o daños o robos de que puedan ser objeto los bienes asegurados a través del contrato.

7. Uso en actividades relacionadas con la seguridad nacional: aunque es un tema un tanto ambiguo, situaciones relacionadas con la seguridad de un estado pueden tomar como base la información obtenida a través del análisis forense digital.

8. Usos en la investigación científica: las mismas organizaciones que se ocupan del desarrollo de procedimientos, protocolos y herramientas de seguridad informática, emplean el análisis digital forense como herramienta de investigación.

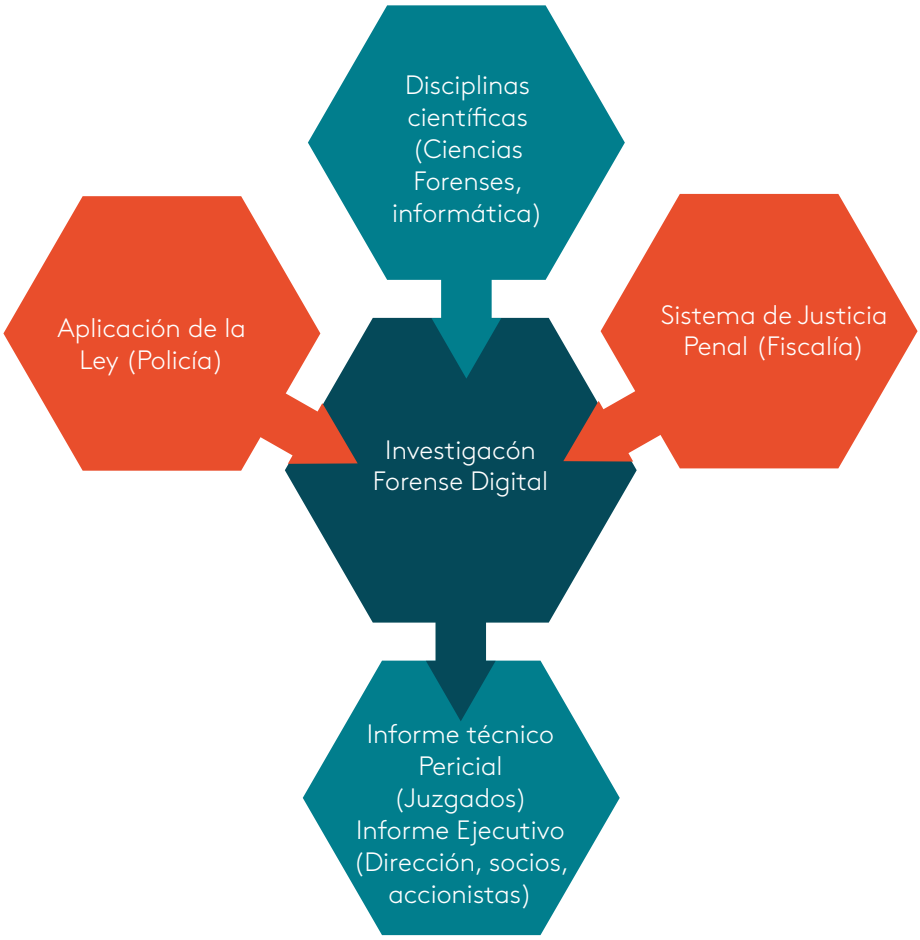


Figura 1. Factores que inciden en la investigación digital forense
Fuente: Kennedy, 2008

No todos los tipos de investigación descritos en los numerales anteriores deben atender de forma estricta cada uno de los pasos de la investigación forense, pero siempre que los elementos sean aportados y analizados como prueba dentro de un proceso judicial o una investigación interna deberán cumplir con todos y cada uno de los pasos previstos, tanto en la cadena de custodia como en el ciclo de la investigación forense.

Es necesario aclarar que las múltiples aplicaciones que encontramos en la actualidad en los sistemas de procesamiento automático de información, y su uso predilecto como herramienta de comunicación, hacen que las redes y dispositivos no solo sean blanco de

ataques para obtener información, también las actividades o conversaciones que sostiene pueden ser objeto de escuchas (legales o ilegales).

Para mayor información consulte en la página principal del eje la videocápsula.

Video

Edward Snowden en eldiario.es - primera parte.

https://www.youtube.com/watch?v=Glz2AqqDxao

Así, el campo del análisis forense abarca múltiples escenarios que, por encima de las consideraciones técnicas y de

conocimientos para su desarrollo, exigen que el investigador observe de forma cuidadosa la legislación vigente en el territorio en el cual adelanta su trabajo.

Video

Para complementar su formación lo invitamos a consultar en la página principal del eje, la video cápsula ***7 consejos de Snowden para evitar ser espiado en internet***.

Derechos fundamentales de los ciudadanos

Figura 2. Derechos fundamentales
Fuente: propia

Uno de los temas que puede causar mayor impacto a una investigación digital forense es el relacionado con la posible vulneración de algún, o algunos de los derechos fundamentales del ciudadano o ciudadanos vinculados bajo alguna de las figuras legales en una investigación, así las naciones suscriptoras de la carta de las Naciones Unidas, acogen la ***Declaración Universal de los Derechos Humanos*** que plantea unos derechos básicos para los habitantes de cualquiera de las naciones suscriptoras del acuerdo. De la carta destacamos los siguientes artículos que se relacionan de forma directa con el campo de acción del investigador digital forense:

Artículo 2°: consagra la igualdad de derechos de todas las personas en todas las naciones, sin distinción de color, raza, credo, filiación política o cualquier otra condición susceptible de ser tomada como base para discriminación.

Artículo 7°: proclama la igualdad ante la ley de cualquier persona sin ningún tipo de discriminación o distinción en virtud de su persona, y pone a los ciudadanos bajo la protección de las leyes.

Artículo 8°: concede a las personas la facultad de acceder a recursos efectivos dentro de la ley y ante tribunales que las protejan contra la vulneración de sus derechos fundamentales consagrados en la Constitución Política.

Artículo 10: consagra el derecho fundamental de las personas a ser escuchadas en igualdad de condiciones como parte de cualquier proceso legal.

Artículo 11: consagra la presunción de inocencia de cualquier individuo a quien se impute la comisión de un delito o falta, hasta que se compruebe su culpabilidad en un juicio legal, además se debe proveer al individuo de las garantías suficientes para su defensa. Dispone que ninguna persona puede ser objeto de pena o sanción o condena por una falta o delito que en el momento de su ocurrencia no se encontraba tipificada en los códigos.

Artículo 12: este es tal vez uno de los derechos que se relaciona de forma más directa con la labor de la investigación digital forense, en él se consagra que ningún ciudadano puede ser objeto de ningún tipo de intromisión en su vida privada, o de su familia, o de su domicilio, o de su correspondencia, ni podrá recibir ataques contra su honra o reputación. La ley debe proveer los mecanismos necesarios para proteger a las personas de estas intromisiones o ataques.

Así los países suscriptores de la carta de las Naciones Unidas, dentro de ellos Colombia, deben expedir leyes que observen los Derechos Humanos, como parte de los derechos fundamentales de sus ciudadanos.

De este modo en el ámbito de la Constitución Política de cada una de las naciones, se deben consagrar como derechos de los ciudadanos los registrados en la declaración de la ONU; según la Organización de las Naciones Unidas en el año 2011, ciento noventa y dos (192) naciones hacen parte de la organización.

En nuestro país, la Constitución Política de 1991, consagra los derechos fundamentales de los ciudadanos, el Capítulo I de la carta fundamental "De los Derechos Fundamentales" en sus artículos 11 a 41, consagra los derechos fundamentales de los ciudadanos colombianos, destacamos aquí los que se encuentran relacionados de forma directa con la investigación digital forense, pero antes le invitamos a realizar la actividad de repaso:

Instrucción

Usted como investigador digital forense debe atender algunos casos en los que en apariencia se está usando los correos electrónicos para adelantar actividades ilícitas, como extorsión y lavado de activos, ¿qué consideraciones de carácter legal debe observar para acceder a los correos electrónicos de víctimas y/o victimarios?

1. El fiscal presenta para que usted lo analice el correo electrónico personal de una mujer acusada de extraer sin autorización una base de datos de clientes de la compañía y asegura que a través del correo ha enviado a un destinatario externo información relacionada con los clientes.

a. ¿Qué requisitos de carácter legal deben cumplirse para que usted pueda acceder a analizar los correos, sin correr el riesgo de que su intervención sea declarada ilegal?

b. ¿Está incurriendo el fiscal en una violación al derecho de la mujer a la "intimidad"? Argumente su respuesta.

c. ¿Existe algún procedimiento de carácter técnico que pueda asegurar la integridad de la bandeja de entrada y salida de un correo electrónico ofrecido por proveedores como Google, Outlook o Yahoo!? Explique su respuesta.

2. Un empleado de una empresa ha usado el correo electrónico corporativo para en apariencia extraer información confidencial sin autorización, usted es contratado por la empresa para recuperar y hacer una copia de seguridad de los archivos contenidos en el servidor de correo para usarlos como evidencia.

a. ¿Requiere alguna autorización especial para acceder al servidor y desarrollar las tareas de recolección y adquisición de la evidencia (correos electrónicos enviados y recibidos) en la cuenta del empleado que está siendo investigado? Justifique su respuesta.

b. Luego de desarrollar la tarea, el abogado del investigado entabla una demanda en su contra por violar su derecho a la intimidad. ¿Tiene posibilidad de prosperar la demanda? Desarrolle su respuesta.

c. ¿Por qué un correo electrónico corporativo no se considera una extensión de la órbita personal del usuario? Explique la respuesta.

Artículo 13. Consagra la igualdad de las personas ante la Ley, y establece la obligación del estado de brindarles protección y evitar conductas de carácter discriminatorio, en virtud de cualquier tipo de condición. Además, promueve la especial protección de los ciudadanos en condición de debilidad manifiesta. Este artículo tiene una especial connotación para el investigador digital forense, pues hechos como las conductas discriminatorias a través de redes sociales o dispositivos electrónicos son muy comunes en nuestro territorio.

Artículo 15. Uno de los derechos que con mayor frecuencia debe observar la investigación digital forense, es en especial el consagrado en este artículo, así la Constitución Política establece que toda persona tiene derecho a su intimidad personal, familiar y a su buen nombre, y es obligación del estado propender por su respeto. En este sentido el ciudadano tiene derecho a conocer actualizar y rectificar la información que se haya recogido sobre él en bases de datos, y archivos de entidades de carácter público y privado.

Consagra además el artículo 15 la inviolabilidad de la correspondencia y demás formas de comunicación, y regula su interceptación o registro a través de orden judicial y bajo el estricto cumplimiento de las formalidades que establece la ley. La reglamentación del derecho a la información y el buen nombre en bases de datos se encuentra consagrada en la Ley 1266 de 2008, conocida como "Ley de Hábeas Data", de esta norma hablaremos más adelante.

Artículo 20. Consagra la libertad de expresión y difusión de pensamientos e ideas, además faculta a los ciudadanos a fundar medios masivos de comunicación.

Artículo 25. Promulga el derecho al trabajo, el estado está en la obligación de promoverlo y protegerlo.

Artículo 29. Establece como derecho fundamental de todos los ciudadanos el "Debido Proceso", así, en cualquier tipo de actuación de carácter judicial o administrativo se deben observar procedimientos estrictos que aseguren este derecho. El debido proceso es uno de los derechos fundamentales que por acción u omisión del investigador digital forense afecta las investigaciones y en un elevado número de casos impacta de forma negativa la investigación; así por vulnerar este derecho, muchas investigaciones que demuestran la responsabilidad del investigado en la comisión de un delito, no se aceptan como prueba por la administración de justicia.

¡Reflexionemos!

¿Qué responsabilidad puede recaer en el investigador digital forense que por no cumplir la cadena de custodia afecte el resultado de una investigación relacionada con el homicidio de una persona?

La protección de datos personales

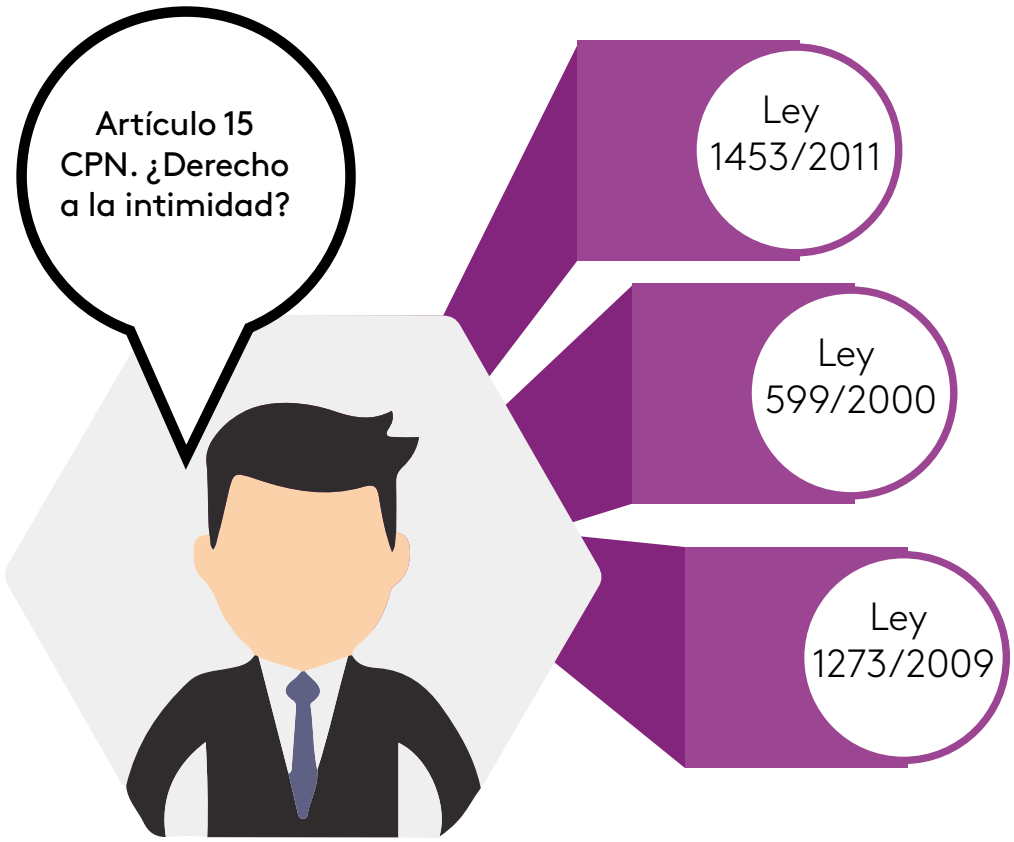


Figura 3. Intimidad
Fuente: propia

En cumplimiento de las obligaciones consagradas por la constitución al Estado colombiano en relación con la garantía de los derechos fundamentales de los ciudadanos, se han promulgado dos leyes generales bajo la figura de leyes estatutarias que reglamentan la forma como se garantizará a los ciudadanos el disfrute de sus derechos, en especial los consagrados en los artículos 15 y 20.

Ley Estatutaria

Leyes de rango superior y tienen carácter prioritario, son las que se expiden para regular la protección de normas de carácter constitucional fundamental.

Ley Estatutaria 1266 de diciembre 31 de 2008

Reglamenta el artículo 15 de la Constitución en lo referente a la honra y buen nombre de los ciudadanos, así como el derecho a la intimidad personal y familiar. En ella se destacan los siguientes artículos relacionados con el área de la investigación digital forense.

Artículo 2°. La ley se aplica a todos los datos de las personas registrados en cualquier base de datos, bien sea de naturaleza pública o particular. Es decir que entidades como las centrales de riesgo crediticias, bancos y cualquier otro tipo de institución que administra información de personas naturales o jurídicas se encuentra obligada a cumplir la reglamentación contenida en ella.

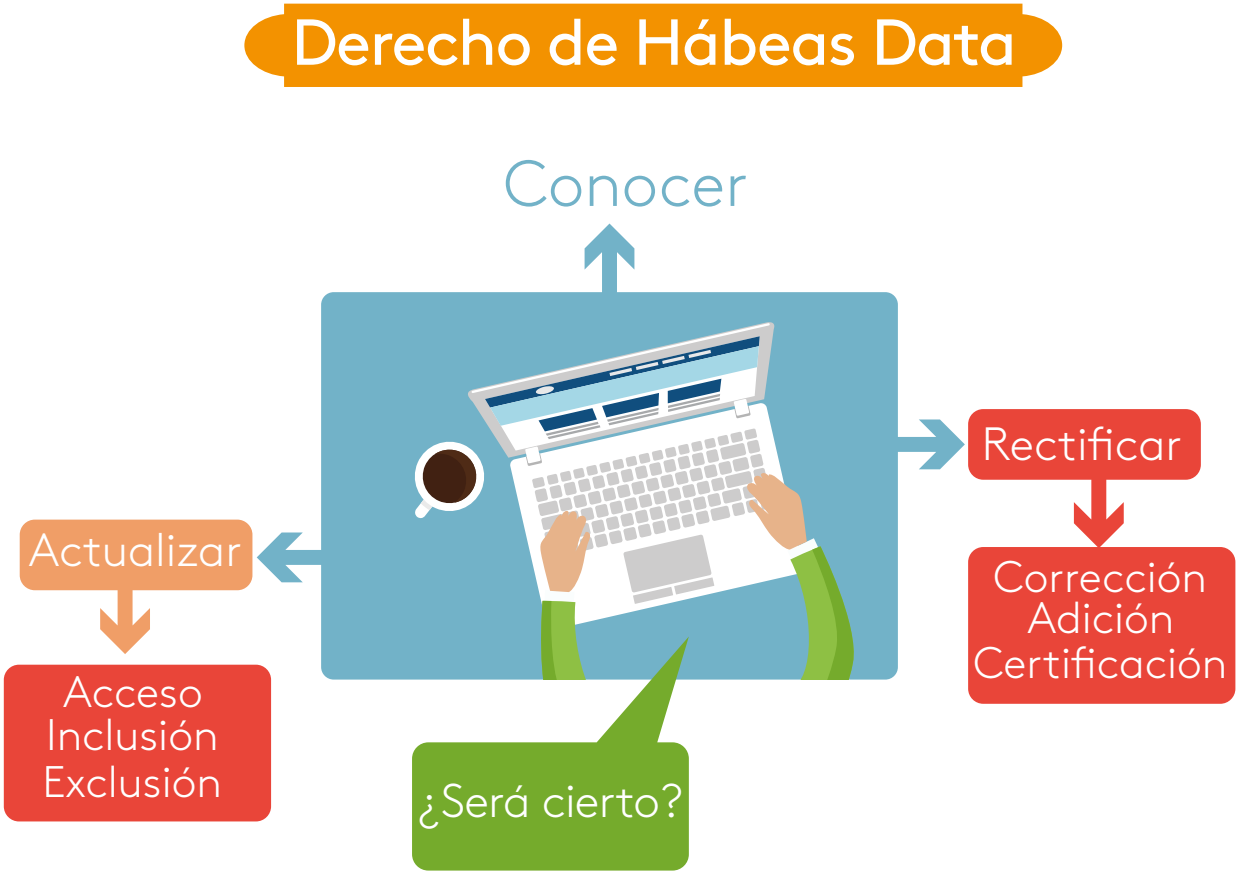


Figura 4. Hábeas data
Fuente: propia

Artículo 3°. Define los siguientes conceptos relativos a la norma:

Titular de la información.

Fuente de información.

Operador de información.

Usuario.

Dato personal.

Dato público.

Dato semiprivado.

Dato privado.

Agencia de información comercial.

Artículo 4°. Principios de administración de datos.

Principio de veracidad o calidad de los datos registrados: la información registrada en las bases de datos debe corresponder con características de veracidad, completitud, exactitud, y debe encontrarse actualizada y ser comprobable y comprensible. La norma prohíbe de forma expresa publicar información fragmentada, incomprensible o no verificable.

Principio de finalidad: debe establecerse e informar al dueño de la información qué propósito tiene la información que estará en esta base de datos para que el titular consienta su uso o publicación.

Principio de circulación restringida: establece que la información del ciudadano registrada en las bases de datos no puede ser de conocimiento de terceros interesados y únicamente podrá ser accesible por la entidad o entidades a las que el ciudadano haya autorizado para acceder o compartir la información.

Principio de temporalidad de la información: cuando la información registrada deja de ser utilizable por quien recibió la autorización, no puede ser suministrada a terceros u otros interesados.

Principio de interpretación integral de derechos constitucionales: la ley se ajusta a los preceptos constitucionales en los temas relacionados con el artículo 15, como son, derecho al buen nombre, el habeas data, derecho a la honra, derecho a la intimidad y a la información.

Principio de seguridad: la información registrada en los bancos de datos, se deberá proteger mediante los diferentes métodos que su tenedor considere necesarios para garantizar su custodia, control de acceso (solo usuarios autorizados), evitar su pérdida y prevenir su adulteración.

Principio de confidencialidad; todas las personas u organizaciones que tengan acceso a la información de los usuarios que no sea considerada de carácter público deben abstenerse de divulgar por algún medio esta información, del mismo modo deben garantizar que una vez terminada la relación con la entidad esta información se mantenga bajo estricto control y solo podrá ser usada en los eventos que la ley determine para este fin.

Artículo 6°. Consagra los derechos de los titulares de la información, de este artículo vamos a destacar que la norma establece tres categorías de datos o información de los usuarios que puede encontrarse en los bancos de datos:

- Información pública.
- Información semiprivada.
- Información privada.

A pesar que el artículo 6° no establece una clasificación adicional, la jurisprudencia emitida por la Corte Constitucional, reglamenta:

> Información reservada: se trata de información personal que se encuentra en estrecha relación con sus derechos fundamentales (dignidad, intimidad y libertad) por esta razón se encuentra ligada a su espacio personal individual y no puede ni siquiera ser obtenida u ofrecida por ninguna autoridad judicial en el desempeño de sus funciones, un ejemplo de esta información es la información genética y lo que la Corte ha llamado "datos sensibles" filiación política del ciudadano, su credo, ideología, inclinación sexual, hábitos entre otros.

Cabe destacar que una de las conclusiones que se pueden obtener del análisis de la jurisprudencia y de la norma en particular, es la inviolabilidad de cualquier forma de comunicación privada, a la cual solo se podrá acceder a través de una orden judicial y bajo las condiciones que la ley determina. En relación con la información registrada en las bases de datos, establece un conjunto de reglas para quienes la administran y consagra unos derechos inalienables para los ciudadanos como el derecho al buen nombre, a la corrección, a la restricción de su uso entre otros. Para finalizar esta sección vamos a realizar la actividad de repaso 2.

Información Pública

En relación con la Ley 1266 de 2008 y la reglamentación vigente la Corte Constitucional en distintas sentencias la ha definido como la que se puede dar u ofrecer sin ninguna reserva, por ejemplo el estado civil de una persona, su edad, su documento de identidad, nacionalidad. En lo general está información se encuentra registrada en su documento de identidad. Corte Constitucional. Sentencia T-414/10.

Información Semiprivada

En relación con la Ley 1266 de 2008 y la reglamentación vigente la Corte Constitucional en distintas sentencias la ha definido como aquella que trata asuntos de carácter personal o impersonal y la norma no la ha definido como pública, por tal razón su acceso solo puede lograrse a través de orden de una autoridad de carácter administrativo, o como parte de los principios de administración de datos personales; por ejemplo las relaciones con entidades prestadoras de servicios de salud, o relacionados con el comportamiento financiero. Corte Constitucional. Sentencia T-414/10.

Información privada

En relación con la Ley 1266 de 2008 y la reglamentación vigente la Corte Constitucional en distintas sentencias la ha definido como la que habla de forma exclusiva de información propia del dominio individual de la persona, y solo se puede obtener u ofrecer a través de orden judicial como parte de un proceso, ejemplos de ella son la información de las historias clínicas de un paciente, los libros de contabilidad, los documentos y correspondencia privados, sus conversaciones telefónicas o digitales, correo electrónico, o la información que se obtenga del ciudadano a partir de una inspección judicial a su domicilio. Corte Constitucional sentencia T-414/10.

Instrucción

El marco normativo vigente en Colombia, en relación con la información y los datos personales, consagra Derechos como el Hábeas Data, a su vez obliga a los proveedores de comunicaciones a mantener una base de datos que registre las comunicaciones sostenidas por los suscriptores por períodos de cinco años, se puede generar entonces una tensión entre los derechos fundamentales y la legislación vigente.

1. De acuerdo a lo reglamentado en la Ley 1266 de 2008 "Ley de Hábeas Data" explique cada uno de los siguientes conceptos relativos a la norma.

a. Titular de la información.

b. Fuente de información.

c. Operador de información.

d. Usuario.

e. Dato personal.

f. Dato público.

g. Dato semiprivado.

h. Dato privado.

i. Agencia de información comercial.

2. Explique cómo se puede garantizar el principio de confidencialidad de la información del ciudadano registrada en una base de datos, si está se comparte entre distintas entidades.

3.Usted como encargado de administrar una base de datos de clientes de una entidad financiera olvida solicitar a los usuarios la autorización para compartir información, un ciudadano recibe una llamada en la que le ofrecen un producto de una empresa en la que nunca ha tenido relación comercial, al preguntar cómo accedieron a sus datos, el interlocutor indica que la obtuvieron a través de su empresa. ¿Se configura un posible delito en la administración de la información que registrada en la base de datos? Si la respuesta es afirmativa, ¿de qué delito se trata y qué consecuencias podría acarrear?

4. Es necesario recordar apreciado investigador que la información que usted registra cuándo hace un trámite ante cualquier entidad entra a formar parte de las bases de datos, las entidades como una simple formalidad le entregan un pequeño documento que autoriza el manejo de su información. ¿Se ha tomado el trabajo de leer lo que está firmando? ¿Si la autorización que usted firma implica información privada o sensible y la entidad la comparte con otros usted cómo se puede defender?

Ley Estatuaria 1581 de 2012

Complementa las definiciones y categorías reglamentadas en la Ley 1266 de 2008 y amplía la clasificación de los tipos de base de datos sobre los que existe un tratamiento especial así:

- Bases de datos o archivos del ámbito personal o doméstico.

- Bases de datos y archivos que tienen como fin preservar la seguridad nacional, prevenir y monitorear el lavado de activos y financiación de actividades terroristas.

- Bases de datos con información de inteligencia y contrainteligencia.

- Bases de datos y archivos de investigación periodística.

- Bases de datos y archivos regulados por la Ley 1266 de 2008.

- Bases de datos y archivos regulados por la Ley 79 de 1993.

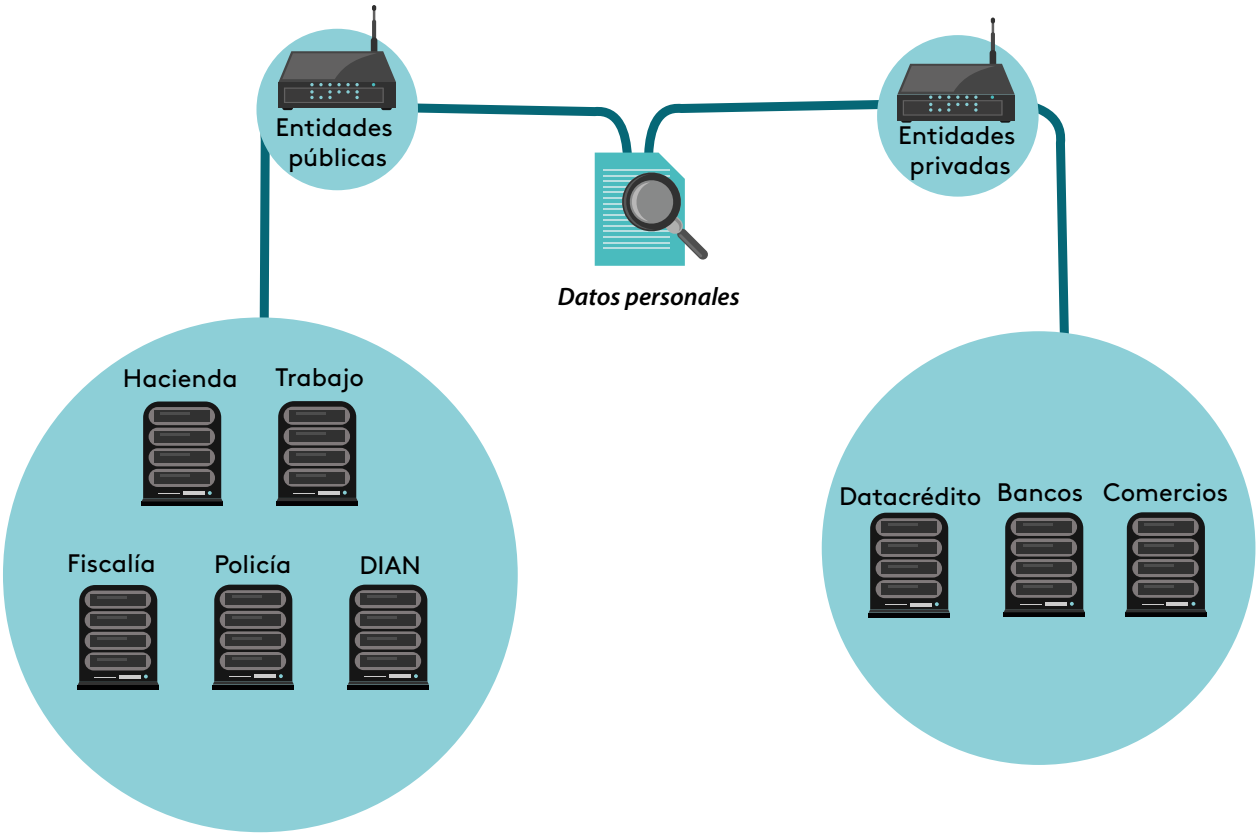


Figura 5. Bases de datos
Fuente: propia

El título III de la Ley Estatuaria 1581 de 2012 establece las categorías especiales de datos entre los que se destacan:

Artículo 5°. Datos sensibles: todos los que afectan de forma directa o indirecta la intimidad del titular, o cuya divulgación o uso pueden afectar su intimidad, por ejemplo, sus inclinaciones sexuales, convicciones, información relacionada con su salud, credo, origen étnico, filiación política, pertenencia a grupos de defensa de derechos humanos.

Esos datos solo pueden ser tratados bajo las siguientes situaciones:

• Autorización expresa del titular referida con exclusividad a dicho procedimiento, con excepción de casos en los que la ley exime de la autorización del titular para su uso. Ejemplo una solicitud de un juez por estar vinculado el individuo en calidad de sindicado en una investigación judicial.

• Acceder a esta información sea necesario para salvaguardar la vida del titular y él se encuentre en incapacidad física o jurídica para hacerlo, en este caso su representante legal, cónyuge o familiar en primer grado de consanguinidad debe autorizar su uso.

• Uso expreso por una organización no gubernamental u organización sin ánimo de lucro de carácter sindical, o política o religiosa, pero de forma exclusiva relacionada con la información de sus integrantes. No se pueden compartir con terceros sin autorización expresa del titular.

• Se requiera su uso para el ejercicio de la defensa o reconocimiento de un derecho en un proceso judicial.

• Se use con fines históricos, estadísticos o científicos, se podrán recabar los datos para estos fines, pero ocultando la identidad de la persona.

Artículo 7. Queda prohibido de forma expresa por la Ley la difusión, uso o publicación de los datos de los menores de edad, niños, niñas y adolescentes. Solo pueden ser tratados los datos que tienen carácter público.

Artículo 10. No se requiere la autorización previa del titular de los datos en los siguientes eventos:

• Información que una entidad pública o administrativa solicite como parte de sus funciones, por ejemplo, verificar la información de SISBEN de un ciudadano para verificar si cumple las condiciones para acceder a los beneficios.

• Orden o requerimiento judicial: la solicitud debe ir firmada por un juez de la república.

• Información pública.

- Urgencias médicas o de salud pública.

- Uso para fines estadísticos o históricos.

- Información del registro civil.

El responsable, o las organizaciones responsables de administrar las bases de datos de información, están en la obligación de informar al titular sobre el requerimiento que se haya realizado para tal fin y la entidad o autoridad que solicita.

Establece, además la Ley 1266, los derechos y condiciones que revisten de legalidad el tratamiento de datos personales, los procedimientos para consultas y reclamos, los deberes de los responsables de las bases de datos y los encargados del tratamiento de la información y asigna a la Superintendencia de Vigilancia la responsabilidad de velar porque lo contenido en la norma se haga efectivo en el manejo de la información de las personas que se encuentran registrados en cualquier tipo de base de datos independiente de su naturaleza pública o privada.

Algunas normas contempladas en esta Ley se reglamentan a través del Decreto 1377 de 2013.

Hasta este punto revisamos grosso modo la legislación relacionada con los derechos fundamentales de los individuos, la forma como se deben administrar las bases de datos que contienen información de los ciudadanos y la clasificación de los datos conforme a la legislación vigente.

Se estará usted preguntando; ¿qué pasó con los delitos, y crímenes que se realizan a través de sistemas de procesamiento automático de información y la investigación relacionada con el hombre que acosa a su ex pareja amenazando con publicar fotos íntimas?

Como hemos precisado en párrafos anteriores, es necesario destacar que, en relación con las normas, la legislación vigente en los países determina la existencia de dos ramas generales del derecho; el derecho civil y el derecho penal; así el primero regula las relaciones de las personas naturales que hacen parte de una sociedad, que se encuentran registradas en el código civil. De otra parte, el derecho penal en su sentido más amplio, tiene como objeto sancionar comportamientos humanos que no se adaptan al sistema normativo, que protege los bienes que dan fundamento a las sociedades, comportamientos que se convierten en infracciones a las normas y a los bienes jurídicamente protegidos por el Estado (se consideran bienes jurídicos bajo la protección del Estado, la vida, la honra, la libertad, el derecho a la propiedad privada entre otros).

La Organización de las Naciones Unidas ONU (2013) en su exhaustivo estudio sobre el delito cibernético, pone de manifiesto las dificultades que puede afrontar la investigación digital forense y la seguridad de la información en relación con la efectividad de la justicia penal, cabe destacar que en esta categoría, hablamos además de investigación, acusación, e imputación de delitos realizados contra sistemas de procesamiento automático de información, o realizados a través de ellos, además abarca la adquisición de evidencia forense digital relacionada con cualquier tipo de delito para adelantar investigaciones de carácter penal.

¡Recordemos que!

Es oportuno recordar que la conectividad de los sistemas de procesamiento electrónico de información en diferentes tipos de redes con cobertura mundial, hace que los delitos relacionados con la investigación digital forense puedan adquirir un carácter transnacional, según la ubicación geográfica (o lógica) de los equipos que efectúan el ataque y de los equipos atacados. esta condición sumada a la volatilidad de la evidencia digital exige un trabajo conjunto entre las administraciones de justicia de diferentes naciones para acometer con éxito la investigación.

Ley 527 de 1999

En agosto de 1999, el Estado colombiano promulga la Ley mejor conocida como Ley de servicios de la sociedad de la información y del comercio electrónico, que entre otros aspectos se destaca porque aplica normas, términos y procedimientos relacionados con el Derecho a un área que para el momento era novedosa y revestía total desconocimiento para las autoridades en materia de investigación y en términos judiciales; de esta Ley se destaca que aplica por primera vez el derecho probatorio a las tecnologías de la información y las comunicaciones y se aplica a cualquier información que se presente en forma de mensaje de datos. Puede consultar la ley en la página principal del eje. En esta ley consideramos:

Mensaje de datos

Información generada, enviada, recibida, almacenada o comunicada a través de medios electrónicos, ópticos, o similares, pueden ser a través de fax, telefax, medios ópticos, internet, correo electrónico, telegramas entre otros.

Ley 527 de 1999.

Artículo 10. Reconoce al valor de los mensajes de datos como prueba en un proceso judicial, no exige que necesariamente el mensaje se encuentre en su forma original, puede presentarse ante el juez una transcripción, pero observando en todo momento la formalidad de la cadena de custodia y demás procedimientos mencionados en el desarrollo del eje epistemológico. La clasificación de los documentos admisibles como prueba ha sido reglamentada a través del artículo 251 del Decreto 1400 de 1970, "por el cual se expide el código civil".

Artículo 11. Determina la forma como se asignará valor probatorio a los mensajes de datos, es decir los criterios que debe reunir el mensaje para ser admitido como prueba, se destaca el uso de la regla de la sana crítica, además, hace énfasis en la confiabilidad que debe caracterizar todas las etapas de proceso de la prueba, desde su recolección, adquisición, conservación, análisis y demás instancias que afronta una evidencia digital desde el momento de la intervención del investigador digital forense. Vale aclarar respetado investigador que usted conoce ya cada uno de estos elementos destacados en el ciclo de la investigación digital forense y en la cadena de custodia.

Sana Crítica

Término usado en derecho para hacer referencia al proceso de emitir un juicio partiendo de la veracidad de los hechos presentados, sin vicios ni errores a partir del raciocinio lógico, la dialéctica, la experiencia del juez y bajo la ayuda de ciencias y artes afines y la moral de los implicados para alcanzar a través de expresión motivada la certeza sobre la prueba que se presenta en el proceso.

Artículo 41. Asigna a la superintendencia de industria y comercio la responsabilidad de vigilar, controlar y regular todas las actividades relacionadas con el comercio electrónico, las firmas digitales, las entidades certificadoras y demás actividades relacionadas con las disposiciones contenidas en la Ley.

En consecuencia con la rápida incursión de las tecnologías de la información y las comunicaciones en el país, así como la veloz aparición de múltiples aplicaciones y herramientas para promover la conectividad entre distintos tipos de dispositivos, los crímenes cometidos a través de dispositivos electrónicos de procesamiento de información presenta un significativo incremento, situación que afecta de forma considerable el desarrollo económico del país, en especial gracias al uso de las tecnologías de la información y las comunicaciones no solo para ayudar en los negocios, también como una nueva fuente de negocio.

Participación de los medios utilizados para realizar operaciones bancarias Colombia 2013

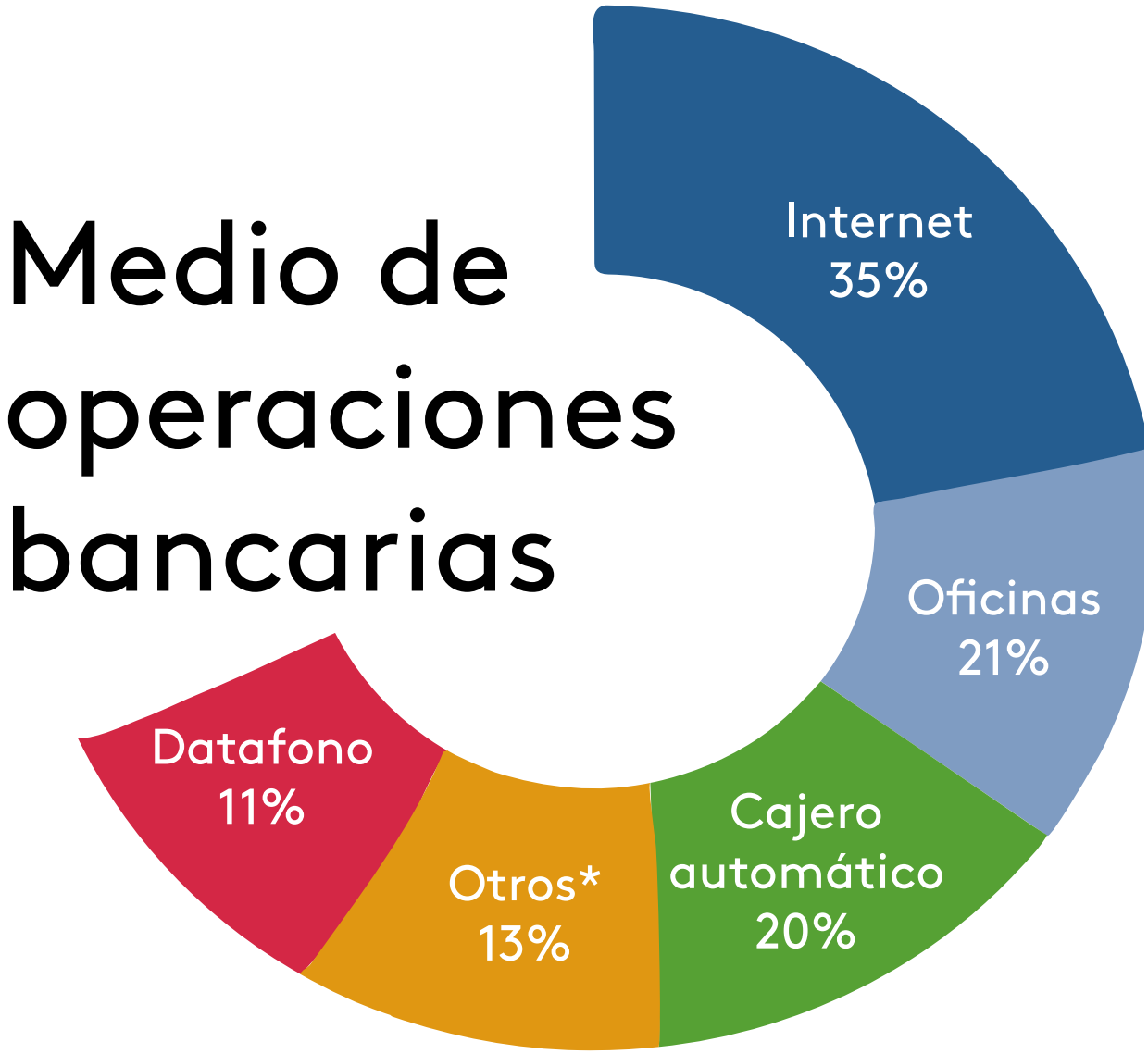


Figura 6. Medio de operaciones bancarias.
Fuente: Unión internacional de tecnología y Superintendencia financiera

La tendencia muestra como para el año 2009 un elevado porcentaje de usuarios del sistema financiero en Colombia prefiere realizar las actividades relacionadas con sus transacciones financieras a través de Internet, por tal razón durante el año 2009 se expide en Colombia la Ley 1273 de 2009, a continuación, señalamos sus aspectos más relevantes.

Ley 1273 de 2009

La expedición de esta Ley marca un hito importante en la historia de la informática forense en Colombia y en el ámbito de la investigación digital forense; crea un nuevo bien jurídico, que hasta el momento no estaba definido en la Constitución Política Nacional; se crea así entonces el bien jurídico tutelable denominado "de la protección de la información y los datos".

Tutelable

Hace referencia a un derecho fundamental, consagrado en la Constitución Política Nacional a través de artículo 86. Así, cuando un ciudadano considera que se está vulnerando uno de sus derechos fundamentales consagrado en la constitución, puede recurrir a la acción de tutela para reclamar l restablecimiento del derecho.

Ésta norma es la piedra angular sobre la que debe reposar cualquier análisis forense que sea de su responsabilidad apreciado investigador, y en consonancia con el bien jurídico creado, expide un conjunto de reglas, destinadas a preservar de forma integral los sistemas que emplean tecnologías de la información y las comunicaciones. De esta Ley se destacan entre otros los siguientes artículos:

> Artículo 1; adicional al Código Penal Colombiano un nuevo Título, el VII BIS y lo denomina "de la Protección de la información y de los datos".

A partir del anterior numeral, se retoma la numeración consecutiva del Código Penal a partir del artículo 269A (Se conserva la numeración original del Código Penal y las letras corresponden a los artículos que se adicionan por la Ley 1273).

Artículo 269 A: Acceso abusivo a un sistema informático.

Artículo 269 B: Obstaculización ilegitima de sistema informático o red de telecomunicaciones.

Artículo 269 C: Interceptación de datos informáticos.

Artículo 269 D: Daño Informático.

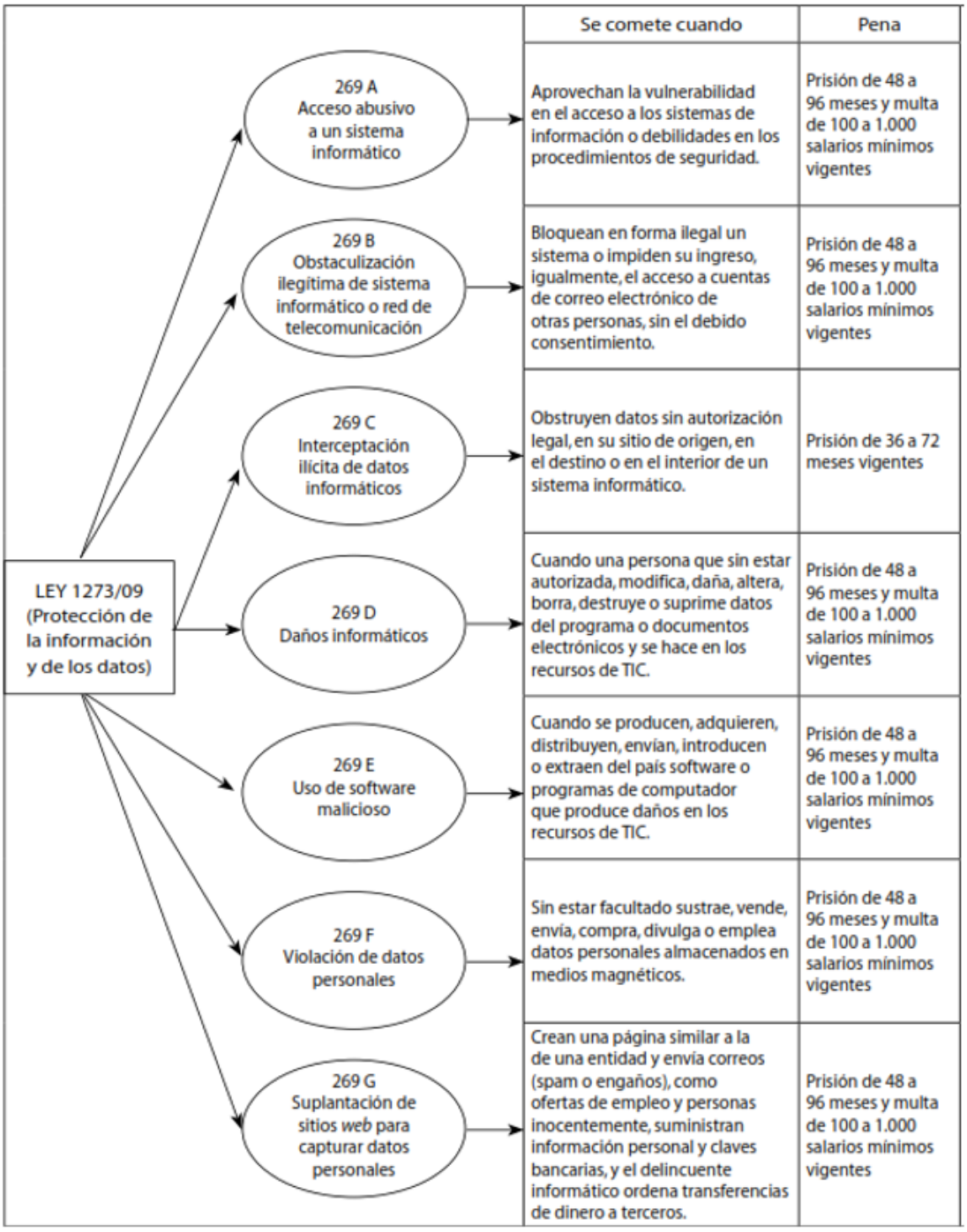
Artículo 269 E: Uso de software malicioso.

Artículo 269 F: Violación de datos personales.

Artículo 269 G: Suplantación de sitios Web para capturar datos personales.

Artículo 269 H: Circunstancias de agravación punitiva.

La figura representa la estructura de la Ley 1273 de 2009 y las sanciones que corresponden a las infracciones a las normas, asociadas al código penal.



Se comete cuando	Pena
Aprovechan la vulnerabilidad en el acceso a los sistemas de información o debilidades en los procedimientos de seguridad.	Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes
Bloquean en forma ilegal un sistema o impiden su ingreso, igualmente, el acceso a cuentas de correo electrónico de otras personas, sin el debido consentimiento.	Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes
Obstruyen datos sin autorización legal, en su sitio de origen, en el destino o en el interior de un sistema informático.	Prisión de 36 a 72 meses vigentes
Cuando una persona que sin estar autorizada, modifica, daña, altera, borra, destruye o suprime datos del programa o documentos electrónicos y se hace en los recursos de TIC.	Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes
Cuando se producen, adquieren, distribuyen, envían, introducen o extraen del país software o programas de computador que produce daños en los recursos de TIC.	Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes
Sin estar facultado sustrae, vende, envía, compra, divulga o emplea datos personales almacenados en medios magnéticos.	Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes
Crean una página similar a la de una entidad y envía correos (spam o engaños), como ofertas de empleo y personas inocentemente, suministran información personal y claves bancarias, y el delincuente informático ordena transferencias de dinero a terceros.	Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes

Figura 7. Ley 1273 de 2009
Fuente: Ojeda, et ál.

Código penal colombiano

La Ley 599 de 2000 por la cual se expide el Código Penal, promulga los delitos, su tipificación y las penas relacionadas con ellos, su expedición en una época en que el uso de las tecnologías de la información y las comunicaciones aún era incipiente, implica que algunos delitos relacionados con las comunicaciones y delitos digitales no hubiesen sido incorporados en el marco penal que se establece a través del código. Sin embargo, a través de leyes de expedición reciente, como la Ley 1453 de 2011 se expide un renovado marco reglamentario que complementa los aspectos que no se tuvieron en cuenta en la expedición del Código Penal.

Ley 1453 de 2011

En su artículo 52, faculta a la Fiscalía General de la Nación a efectuar la interceptación de cualquier tipo de comunicaciones, ya se haga a través de redes públicas o privadas, con el propósito de encontrar materiales probatorios o cualquier tipo de evidencia para personas que puedan aparecer vinculados en la comisión de algún acto ilegal, puede ser en calidad de indiciado, o imputado. Además otorga facultades a las autoridades competentes de efectuar la operación técnica de la interceptación y de procesarla.

Este artículo despierta una gran preocupación en el ámbito de la protección del derecho a la intimidad porque genera un campo de acción muy amplio para las "autoridades competentes" sin especificar qué tipo de autoridades, qué fin, por qué razón o quien autoriza la interceptación. De lo anterior se puede deducir apreciado investigador que bajo lo que se establece en este artículo, todos absolutamente todos nosotros podemos ser objeto de interceptación de nuestras comunicaciones sólo por sospecha. A través del Decreto 1704 de 2012, que reglamenta el artículo 52 de la Ley 1453, de esta norma se destaca:

Artículo 2°: obliga a los proveedores de cualquier servicio de telecomunicaciones en Colombia a incluir como parte de su infraestructura los equipos, plataformas y dispositivos que hagan posible que la fiscalía o la policía judicial puedan acceder a cualquier tipo de comunicaciones que cursen por sus redes. Además, establece la obligación de los operadores de atender con diligencia los requerimientos de las autoridades en relación con la interceptación de las comunicaciones.

Indiciado

Termino relativo al derecho y a la investigación penal, cuando el ente investigador, en este caso la fiscalía, tiene sospechas de la participación de un ciudadano en la participación de alguna actividad ilegal, lo vincula a esta en calidad de indiciado. Es decir hay algunas pistas que señalan que puede tener relación con la comisión del delito.

Imputado

Termino relativo a una investigación realizada por el ente investigador, en el cual al ciudadano se le atribuye la comisión de un delito, en este caso a través de las evidencias pasa de ser indiciado a ser imputado (acusado) del delito.

Interceptación

En lo referente a las telecomunicaciones, hace referencia a la actividad según la cual a través de dispositivos tecnológicos, se accede a una red de comunicaciones (con o sin autorización) y se obtienen los datos de una determinada transmisión, o llamada. Por lo general el dueño de la comunicación desconoce que está siendo interceptado.

Artículo 4°: obliga a los proveedores de comunicaciones a establecer con precisión todos los datos de ubicación relacionados con los suscriptores, identidad, dirección de facturación, disposición de direcciones IP usadas por el suscriptor durante una conexión entre otros datos de carácter privado.

Artículo 5°: exige a los proveedores de comunicaciones suministrar a la fiscalía o autoridades de investigación la ubicación exacta de coordenadas, mallas, sectores, potencia y línea de tiempo de una conversación o transmisión realizados a través de sus redes.

¡Importante!

Es necesario destacar que en Colombia algunas situaciones relacionadas con la evidencia digital forense y la tensión con los derechos fundamentales se han contemplado como parte de la Jurisprudencia expedida por la Corte Suprema de Justicia y la Corte Constitucional, así, por ejemplo la Sentencia 2007-230 "Pruebas con Documento Electrónico" (lo invitamos a realizar la lectura en la página principal del eje) de la Corte Suprema de Justicia define el carácter de las pruebas y su validez bajo el siguiente argumento: se considera una prueba como ilícita cuando vulnera o desconoce derechos de carácter fundamental, o si para su obtención se cometió alguna infracción a un derecho fundamental. En la misma sentencia, se define cuando una prueba es "ilegal" o irregular.

De esta sentencia es oportuno destacar cómo el operador judicial, en este caso la Corte Suprema, aborda el derecho a la inviolabilidad de la correspondencia y las demás formas de comunicación privada. En tutela interpuesta por dos ciudadanos que en última instancia llega para su revisión en este tribunal, la Corte sentencia:

> No se puede aludir una violación del derecho a la intimidad y exigir que se declare inválida y se elimine el historial del correo electrónico de los ciudadanos afectados, cuando estas cuentas se encuentran registradas en los servidores de la empresa, puesto que el correo electrónico con el dominio @empresa.com; se entiende propiedad de la empresa y no del funcionario a quien la organización le asigna este casillero electrónico para el desarrollo de sus labores.

Es decir, que las comunicaciones que usted sostenga a través del correo corporativo, líneas telefónicas corporativas o usando dispositivos que a usted le asigna la empresa no se asumen bajo la esfera privada y pueden ser usadas como parte de cualquier investigación inclusive sin mediar autorización judicial.

En otros decretos y resoluciones que reglamentan las comunicaciones y la conservación de datos, se obliga a las empresas que prestan el servicio de comunicaciones en el país a conservar los datos "relativos a las comunicaciones" en sus bases de datos por un período de tiempo mínimo de cinco (5) años, situación que bajo el análisis de algunos expertos como el abogado e investigador Juan Diego Castañeda constituyen una flagrante violación al derecho a la intimidad, puesto que respecto a la conservación de datos de comunicaciones, la mayoría de países del planeta tienen un período máximo de un año, y en Australia el máximo es de dos años, ¿por qué Colombia aplica un plazo tan amplio?

Castañeda (2016), expone una de las situaciones que más preocupa a los investigadores en el tema y son las amplias definiciones que se encuentran en la norma relativa a la retención o conservación de datos relativos a las comunicaciones, pues al definir el término "historial de comunicaciones" no se definen los elementos del historial que se deben conservar, así pues, no solo se trata de los números marcados, también de la duración de la conversación o de la transmisión y su contenido, además apreciado investigador es mi deber recordarle que todos los archivos que envíe o reciba a través de las redes de comunicaciones contienen "metadatos", forman los metadata de los archivos parte de este historial?

Metadata

Los metadatos se pueden interpretar como los datos que hacen referencia a los datos, es decir a información que acompaña a cualquier archivo digital y que contiene entre otras, fecha y hora de creación del original, datos de la computadora en que se crearon, modificaciones, fechas y horas e inclusive en algunos casos los datos de ubicación geográfica de la pc donde se crea el archivo original.

Otra situación que llama la atención del marco normativo en Colombia, es la exigencia que se realizó a los operadores para que implementen herramientas tecnológicas que permitan que en tiempo real y desde las propias oficinas de comunicaciones de la fiscalía o de la policía judicial, se pueda acceder de forma remota a sus plataformas de comunicaciones para interceptar cualquier llamada o transmisión. Además, la norma exige que las compañías de telefonía no efectúen ningún tipo de cifrado sobre las comunicaciones que se efectúan a través de sus plataformas.

Edward Snowden ex analista de la CIA, contratado para el diseño de un software de interceptación de comunicaciones para la Agencia de Seguridad Nacional de los Estados Unidos lo ha explicado con suficiencia; absolutamente todas las comunicaciones que sostenemos a través de redes de comunicaciones son o pueden ser objeto de escucha en tiempo real, y para el caso de Colombia las empresas de comunicaciones deben almacenar esta información de todos los ciudadanos por un plazo de cinco años. Me pregunto entonces: y, ¿el derecho a la intimidad?.

Video

Para conocer cómo se desarrollan los procesos de vigilancia en Internet por favor consulte la videocápsula *¿Cómo nos vigilan en Internet?* En la página principal del eje.

Aquí un interrogante que sugiero discutir con su grupo de dos compañeros: ¿Considera usted que el marco normativo referente a la conservación de las comunicaciones en Colombia respeta el derecho a la intimidad consagrado en la Constitución Política de Colombia? Cada integrante del grupo debe responder y argumentar su respuesta a partir de las normas citadas durante el desarrollo del presente eje. Luego el grupo debe presentar una única respuesta fruto del acuerdo entre sus integrantes, la cual debe estar acompañada de los argumentos que correspondan. De igual forma vamos a realizar la actividad de repaso 3.

Instrucción

La naturaleza legal de una investigación de carácter digita forense, exige que el investigador observe una serie de conductas apegadas a la legislación y a normas judiciales, que de ser omitidas pueden acarrear sanciones incluso de carácter penal, así se trata entonces de identificar qué procedimientos seguir para desarrollar con éxito la investigación sin vulnerar derechos fundamentales de los ciudadanos.

1. Junto a un compañero de curso, desarrollen la siguiente reflexión: ¿consideran que el marco normativo referente a la conservación de las comunicaciones en Colombia (Ley 25 de 2007, Decreto 1704 de 2012, Resolución 0912 de 2008 de la Policía Nacional), respeta el derecho a la intimidad consagrado en la Constitución Política de Colombia? Por favor argumente su respuesta.

2. Con base en la información suministrada en el módulo y el análisis de la imagen 7, puede usted concluir cuál es el estado actual de desarrollo de la investigación digital forense y la prevención de la ciberdelincuencia en Colombia, por favor explique.

3. Un investigador recibe la orden de iniciar un proceso, como primer paso le solicita a la afectada que abra su correo para revisar los mensajes que ha recibido dando apertura formal a la investigación. ¿Acaso está olvidando algo? ¿A partir de los contenidos y conceptos que ya se han desarrollado podemos inferir si la actuación del investigador es correcta? Por favor argumente su respuesta.

¡Importante!

A partir de las características transnacionales que pueden adquirir los delitos relacionados con los dispositivos de procesamiento electrónico de información, En 2016 la Organización de Estados Americanos (OEA) expide el documento conocido bajo el nombre *Ciberseguridad: ¿estamos preparados en América Latina y el Caribe?* **(realicemos la lectura complementaria en la página principal del eje). Expertos mundiales en temas relacionados con la ciberseguridad y la investigación digital forense hacen una revisión en detalle de los aspectos relacionados con esta área en los países en cuestión y el estado de su legislación respecto de la protección de datos personales, el derecho a la información y la tipificación penal de los delitos.**

Así, se expide el informe relacionado con el nivel de madurez de la legislación en relación con la seguridad cibernética. De este modo, para facilitar el éxito en acciones relacionadas con la investigación digital forense por el carácter transnacional que pueden adquirir estos delitos, se hace una revisión de los siguientes componentes que los autores del informe consideran estratégicos para implementar de forma correcta un sistema completo y robusto para asegurar una efectiva protección de la infraestructura, bases de datos, información, bienes y servicios relacionados con las tecnologías de la información y las comunicaciones:

- Política y estrategia.
- Cultura y sociedad.
- Educación.
- Marcos legales.
- Tecnologías.

Para hacer el análisis de las categorías descritas se define uno o más indicadores por cada una de ellas, estos son evaluados a través de una escala que se ha denominado (nivel de madurez); los valores respecto de los cuales se expide la evaluación y las rúbricas respectivas son los siguientes:

Rúbricas

Guías de puntaje o evaluación que describen las características de un producto o tarea en varios niveles de rendimiento, y en relación con lo que se espera como objetivo final.

• Inicial: no se define como estratégico o fundamental el componente a evaluar, se hace evidente la existencia de componentes aislados y existen propuestas de trabajo desarticuladas al respecto.

• Formativo: existe un esquema elaborado y articulado con la participación de varias agencias gubernamentales y posiblemente internacionales.

• Establecido: existe una estrategia definida y unificada que consulta a los diversos sectores de la sociedad civil, define una estructura jerárquica con niveles de responsabilidad y a partir de tendencias históricas y análisis estadísticos elaboran planes y proyectos relacionados con el indicador, promueve el crecimiento de las capacidades del sector en el país.

• Estratégico: se involucran múltiples actores del contexto nacional en la elaboración de las estrategias relacionadas con el indicador, se considera un proceso de planeación estratégica y se aplica en todo el ciclo, por tal razón hay evaluación, retroalimentación y ajustes de forma continua.

• Dinámico: es el máximo y mejor nivel de madurez deseable, asegura la posibilidad de revisar de forma continua la estrategia, la adapta a los cambios que se presentan en el entorno socio político, impulsa el proceso de toma de decisiones de múltiples sectores interesados, y busca promover el acceso, la transparencia y la confianza a todas las partes interesadas.

Es necesario aclarar que en las rúbricas aquí expuestas se buscó incluir de forma amplia las que corresponden a cada uno de los indicadores, pero una revisión en detalle del informe le permitirá identificar que, para cada categoría y cada indicador, existe una rúbrica especifica frente a la cual se expide la valoración en el informe.

La gráfica presenta los resultados obtenidos para Colombia en el informe elaborado por el BID y la OEA.

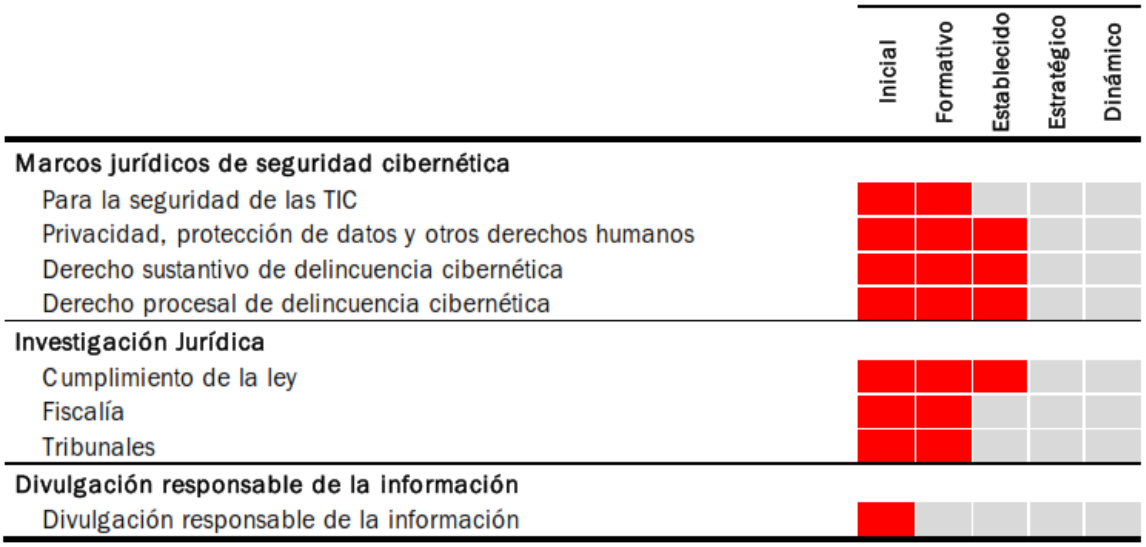


Figura 8. Nivel de madurez
Fuente: BID y OEA 2016

¡Reflexionemos!

Con base en los resultados obtenidos y el análisis del gráfico, ¿puede usted concluir el estado actual de desarrollo de la investigación digital forense y la prevención de la ciberdelincuencia en Colombia?

El crecimiento de las conexiones de banda ancha o fibra óptica en el país, así como el uso cada día más extendido de herramientas digitales de comunicación han abonado el terreno para que personas u organizaciones dedicadas al crimen encuentren en las tecnologías de la información y las comunicaciones un nuevo y prometedor campo de acción lleno de múltiples víctimas potenciales, pues la educación en relación con la protección de información y prevención de amenazas que se realizan a través de redes sociales o Internet es más bien escasa en la mayoría de países.

Figura 9. Evolución banda ancha.
Fuente: Mintic (2015).

La relación entre el aumento de las conexiones de banda ancha en Colombia y el incremento de los delitos relacionados, en este caso particular contra la integridad de los menores de edad, podrá deducirla usted apreciado investigador a través del análisis de la evolución de la banda ancha en Colombia y las denuncias presentadas por la iniciativa Te Protejo 2012-2015.

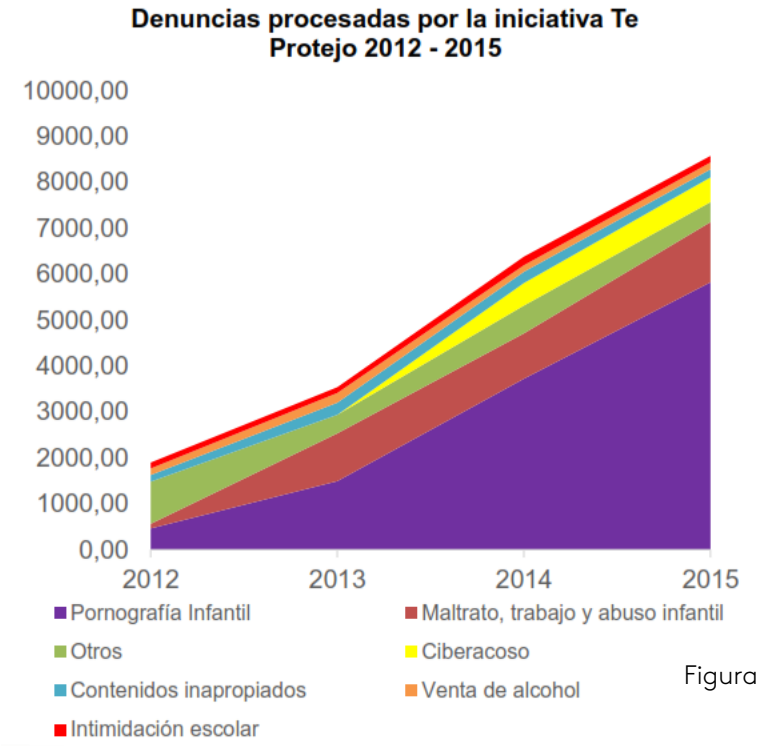


Figura 10. Denuncias procesadas por Te Protejo
Fuente: www. teprotejo.org (2015)

Al respecto es importante mencionar que para el año 2015, el porcentaje de incidentes digitales gestionados por la policía digital en Colombia fueron los siguientes:

Figura 11. Incidentes digitales
Fuente: Conpes 3854 (2016)

El nivel de afectación de los incidentes digitales que se presentó en el país en el año 2015 se puede observar en la siguiente figura.

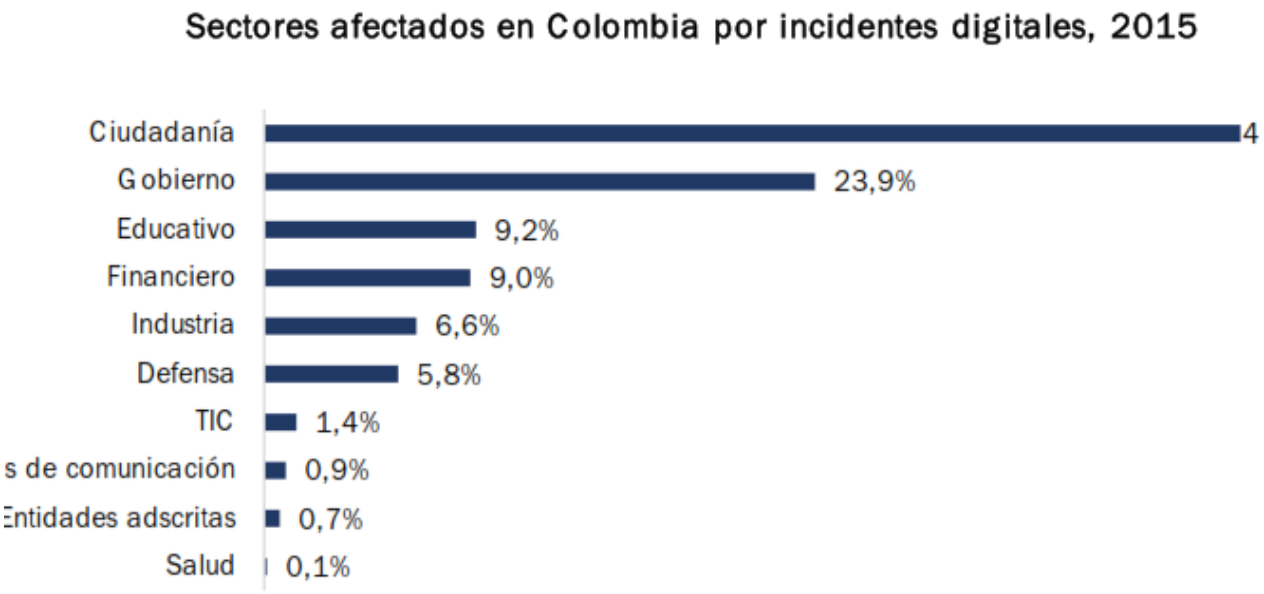


Figura 12. Nivel de afectación
Fuente: Conpes 3854 (2016)

Los resultados que se presentan como parte de este componente, junto a muchos otros provenientes de diversos informes elaborados por la policía nacional, y la fiscalía entre otras entidades son el insumo usado por el Gobierno para expedir en el año 2016 el Documento Conpes 3854, a través del cual se expide la Política Nacional de Seguridad Digital. Así, durante los próximos periodos legislativos se hace prioridad en la expedición de los decretos reglamentarios que abordan su desarrollo.

Los elementos a destacar de la Política de Seguridad Digital en Colombia son:

• Se implementan las estrategias y el plan de acción para desarrollar e implementar la política.

• Se determina un marco institucional para la política de seguridad digital en Colombia, basado en el enfoque de gestión de riesgos.

• Se crean las condiciones necesarias para que las partes y entidades interesadas gestionen los riesgos relacionados con la seguridad digital en sus plataformas tecnológicas y en sus actividades de carácter socio económico y se genere mayor nivel de confianza en el uso de los entornos digitales en el país.

• Implementar estrategias para fortalecer la seguridad de los ciudadanos y del estado en el entorno digital en los ámbitos nacional y transnacional bajo el enfoque de gestión de riesgos.

• Fortalecer la defensa y soberanía nacional en el contexto de la seguridad digital con enfoque de gestión de gestión de riesgos.

• Implementar y desarrollar mecanismos con carácter permanente y estratégico para el fomento de la cooperación, colaboración, y asistencia de seguridad digital, en el contexto nacional e internacional.

• Revisar y valorar de forma continua el impacto económico de la implementación de la política.

El escenario actual de legislación en materia de informática forense puede variar con la misma rapidez con la que evolucionan las tecnologías de la información y las comunicaciones, así cuando se encuentre en el marco de una investigación digital forense revise con cuidado la reglamentación vigente antes de emprender la tarea.

La dificultad para establecer un marco normativo común para perseguir y actuar frente al delito digital, hace muy difícil que delitos que se cometen en un Estado o región puedan ser investigados por las autoridades de otros países en los que pueden estar ubicados los sistemas afectados. Por ejemplo, un grupo delictivo que opera en Australia afecta una red de computadoras ubicada en Colombia y extrae los datos de las bases de datos de un banco cuyo servidor central está en Bogotá, ¿cuál autoridad debe investigar el crimen, la de Australia o la de Colombia; el crimen se cometió en Australia o en Bogotá?

Estos interrogantes y las dificultades relacionadas con definir las competencias de las autoridades se abordan por la Organización Internacional para la Estandarización (ISO por sus siglas en inglés) que en compañía de la Comisión Internacional Electrotécnica (IEC por sus siglas en inglés) emprenden a la tarea de crear un conjunto de normas técnicas de estandarización de alcance mundial, que contribuya a crear estándares relacionados con la investigación digital en todos los países bajo criterios y estructuras semejantes que garanticen la posibilidad de presentar las evidencias obtenidas en cualquier jurisdicción judicial sin temor a que sean rechazadas por las autoridades.

Así, en el año 2012 se expide la primera norma técnica, conocida bajo la referencia ISO/IEC 2037 (2012). Por medio de la cual se expiden los lineamientos para la identificación, recolección, adquisición y preservación de la evidencia digital. Aspectos que fueron contemplados en el desarrollo del eje epistemológico del presente curso. Se espera que este documento haga parte de un conjunto de cinco guías más que buscan estandarizar todos los aspectos relacionados con la investigación digital en el mundo, los demás estándares se encuentran en la actualidad en etapa de desarrollo.

Instrucciones

Apreciado investigador, durante la introducción al presente documento se planteó la pregunta relacionada con una mujer que es víctima de una extorsión que realiza su ex compañero sentimental; ahora a partir de la información que usted conoce con el desarrollo del presente eje, por favor responda la pregunta propuesta en la anteriormente:

¿Acaso está olvidando algo? ¿A partir de los contenidos y conceptos que ya se han desarrollado podemos inferir si la actuación del investigador es correcta? Por favor argumente su respuesta.

BIBLIOGRAFÍA

Organización de las Naciones Unidas. (1945). *Carta de las Naciones Unidas*. Recuperado de http://www.uy.undp.org/content/dam/uruguay/docs/marco-legal-uy/undp-uy-carta-nnuu.pdf

República de Colombia. (1991). *Constitución Política Nacional*. Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4125

República de Colombia. (2008). *Ley Estatutaria 1266 de 2008. Ley de Habeas Data*. Bogotá: Ministerio del Interior y de Justicia.

República de Colombia. (2012). Ley Estatutaria 1581 de 2012. *Ley de Protección de Datos Personales*. Bogotá: Ministerio de las Tecnologías de la Información y las Comunicaciones.

República de Colombia. (2013). Decreto 1377 de 2013. *Por el cual se Reglamenta parcialmente la Ley 1581 de 2012*. Bogotá: Ministerio de las Tecnologías de la Información y las Comunicaciones.

Organización de las Naciones Unidas. (2013). *Estudio Exhaustivo sobre el Delito Cibernético*. Recuperado de: https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Spanish.pdf

República de Colombia. (1999). Ley 527 de 1999. *Ley Servicios de la Sociedad de la Información y del Comercio Electrónico*. Bogotá: Ministerio Comunicaciones.

República de Colombia. (2009). Ley 1273 de 2009. *Ley de la Preservación de la Información y de los Datos*. Bogotá: Ministerio de las Tecnologías de la Información y las Comunicaciones.

República de Colombia. (2000). Ley 599 de 2000. *Por la cual se Expide el Código Penal Colombiano*. Bogotá: Ministerio de Justicia.

República de Colombia. (2011). Ley 1453 de 2011. *Reforma del Código Pena, Código de Procedimiento penal, Código de Infancia y Adolescencia y se Dictan normas sobre Extinción de Dominio*. Bogotá: Ministerio de Justicia y del Derecho.

Corte Suprema de Justicia (2007). Sentencia 2007-230. P*ruebas con Documento Electrónico*. Bogotá: Corte Suprema de Justica.

Castañeda J. (2016). *¿Es Legítima la Retención de Datos en Colombia?. Análisis Comparativo de una Herramienta de Vigilancia Masiva que Restringe los Derechos Humanos*. Bogotá: Fundación Karisma. Recuperado de https://necessaryandproportionate.org/files/2016/05/16/retencion_de_datos_-espanol-.pdf

BIBLIOGRAFÍA

Organización de Estados Americanos (2016). *Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?*. Informe Ciberseguridad 2016. Recuperado de https://publications.iadb.org/handle/11319/7449?locale-attribute=es&

República de Colombia (2016). *Política Nacional de Seguridad Digital*. *Documento CONPES*. *Consejo Nacional de Política Económica y Social*. Departamento Nacional de Planeación.

República de Colombia (2011). *Lineamientos de Política para Ciberseguridad y Ciberdefensa*. Consejo Nacional de Política Económica y Social. Departamento Nacional de Planeación.

Akowuah, F., Yuan, X., Xu, J., & Wang, H. (2013). *A survey of security standards applicable to health information systems*. *International Journal of Information Security and Privacy,* 7(4), 22+. Retrieved from http://go.galegroup.com.proxy.bidig.areandina.edu.co:2048/ps/i.do?p=CDB&sw=w&u=fuaa&v=2.1&it=r&id=GALE%7CA381836143&asid=9b863a32326a9a2b0258d84403a68704