## RESUMEN

La prueba documental electrónica en el proceso penal es frecuente debido a la popularización de las tecnologías de la Información o Comunicación TIC´S, es por esta razón que los procedimientos para su recolección, examen y análisis requieren conocimientos y criterios técnicos, distintos a los usados en la prueba documental soportada en papel.

Estos procedimientos requieren de técnicas especiales aplicadas en las etapas preprocesales de investigación y de instrucción fiscal, que traten de conservar el documento sin alteraciones, y que garanticen su integridad, autenticidad y reproducción, principios importantes para la valoración de la prueba ante el Tribunal de Garantías Penales, ya que la prueba que cuente con estos elementos puede sustentar una resolución. También es de vital importancia que los métodos utilizados para su recolección garanticen los derechos constitucionales y legales, tales como los de secreto de las comunicaciones, correspondencia virtual y protección de datos.

La intervención de un perito se vuelve trascendente, ya que por la complejidad de la prueba es necesario contar con un auxiliar de la justicia que determine y permita que el documento electrónico cuente con los principios enunciados.

**PALABRAS CLAVES**

Prueba electrónica documental, Recolección de evidencias electrónicas, Intercepción de mensajes de datos, Prueba pericial electrónica, Testimonio del perito, Integridad del documento electrónico, Autenticidad del documento electrónico, Reproducción del documento electrónico

# INDICE

UNIVERSIDAD DE CUENCA
**FACULTAD DE JURISPRUDENCIA Y CIENCIAS POLÍTICAS Y SOCIALES**

**DIPLOMADO EN DERECHO PROCESAL PENAL**

# LA PRUEBA ELECTRÓNICA DOCUMENTAL EN EL CÓDIGO DE PROCEDIMIENTO PENAL ECUATORIANO

TESIS PREVIA A LA OBTENCIÓN DEL GRADO DE DIPLOMADA EN DERECHO PROCESAL PENAL

**Autora:**
Dra. Mónica Josefina Jara Villacís

**Directora**:
Dra. Lourdes Álvarez Coronel

CUENCA, ABRIL DE 2010

La responsabilidad por los hechos, ideas y doctrinas, expuestos en este trabajo, corresponden exclusivamente al autor.

Mónica Josefina Jara Villacís

Dedico el presente trabajo:

A mi familia

## AGRADECIMIENTOS

A todos quienes forman parte de mi vida.

Un profundo y sincero “Gracias”.

## INTRODUCCIÓN

Con el advenimiento de las tecnologías de información y comunicación (TIC) y la generalización de su uso en la sociedad del siglo XXI, se han producido cambios sustanciales en las relaciones económicas y sociales, debido a que se han incorporado estas nuevas tecnologías como medios de comunicación y producción, brindando una mayor eficiencia y eficacia en la generación de bienes y servicios, así como en la comercialización de los mismos.

Por la generalización en el uso de las Tecnologías de la Información y Comunicación, se han provocado impactos en todos los sectores sociales y económicos, incluso por medio de ellas se pueden cometer ilícitos, ser sus blancos o dejar sus huellas; misaos que se convierten en evidencias importantes dentro del proceso de investigación penal.

El uso de los documentos electrónicos es generalizado, en todo momento enviamos y recibimos mails, mensajes de celular o SMS, creamos documentos en el computador, subimos comentarios a una página web, almacenamos información en los celulares, aifons, memorias flash, CD, etc.

Esta información en formato electrónico es la que se denomina documento electrónico o mensaje de datos, y requiere ser comprendida no en la forma tradicional, sino es necesario concepciones nuevas sobre su significado, tipos, clases y formas de concepción sobre su originalidad y copias, la existencia de los instrumentos públicos electrónicos, seguridades, etc.

Los documentos electrónicos pueden constituir evidencias de delitos tradicionales o electrónicos, develando datos importantes para establecer su existencia y la responsabilidad de una persona; por lo que el Fiscal y la Policía Judicial, deben acudir a la información en este soporte, copiar y examinar con

cuidado con el fin de que la misma no sufra alteraciones, se borre, desaparezca o migre.

También se requiere para su recolección autorizaciones judiciales emitidas por los Jueces de Garantías Penales para que sean legalmente actuadas, cuidando en todo momento no violentar derechos constitucionales como los de secreto de las comunicaciones, correspondencia virtual y protección de datos.

Así mismo, es necesario contar con la intervención de expertos en temas informáticos y/o electrónicos, que permitan garantizar la integridad, autenticidad y reproducción del documento, y ayuden al Fiscal en un primer momento a determinar la existencia de la infracción, perseguir y descubrir a los autores, cómplices o encubridores de este tipo de delitos. Su intervención resulta vital ya en la etapa de juicio, en donde un profesional auxiliar de la justicia explique y ayude a comprender la complejidad de los sistemas informáticos, y la seguridad de un documento electrónico, para que el Tribunal se forme un criterio y pueda sustentar en debida forma un fallo condenatorio o absolutorio.

La novedad, la complejidad, el desconocimiento y la falta de confiabilidad en la prueba electrónica, provoca conflictos en la recolección de este tipo de evidencias por parte de los fiscales, así como en la presentación ante el Tribunal Penal, ya que a los jueces se les dificulta su valoración, porque requieren se demuestre y se haga comprender lo que significa la integridad, autenticidad, reproducción de un documento electrónico, además dentro de un sistema acusatorio oral, la prueba documental esta siendo dejada a un lado debido a problemas en su concepción dentro de este sistema, ya que no es que lo escrito no dejó de tener importancia, sino que su evacuación es diferente, por ello se necesita sea acreditada la información contenida dentro del documento con otros tipos de pruebas, principalmente la testimonial y material, y sobre su autenticidad, integridad y reproducción por medio del testimonio del testigo experto, quien no solamente se debe limitar a hablar, sino ha demostrar gráficamente o de manera práctica al Tribunal sobre sus hipótesis y conclusiones.

Sin embargo, estos requisitos no están desarrollados en el Código de Procedimiento Penal, sino en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y su reglamento, así como en la doctrina, por ello el presente trabajo recopila información que permite entender mejor estos requisitos, y como éstos se cumplen con soluciones técnicas como el uso de firmas electrónicas o digitales, certificados emitidos por entidades acreditadas en el Ecuador, códigos hash, sistemas de encriptación, etc.

El tener claro estos conceptos, ayudará a que el sistema penal en su conjunto se beneficie, ya que muchos de los delitos quedan impunes, por falta de pruebas, ya que varias de ellas no son encontradas o valoradas en debida forma por las autoridades debido a desconocimiento.

# CAPITULO I

# El DOCUMENTO ELECTRÓNICO

## 1.1 EL DOCUMENTO ELECTRÓNICO; GENERALIDADES, ELEMENTOS

El origen etimológico de la palabra “documento” proviene del griego dék, correspondiente al verbo latino docere “instruir” de donde proviene el vocablo documentum, que significa originalmente “lo que enseña, con lo que alguien se instruye”. En el ámbito jurídico el documento es una cosa que sirve para representar a otras; es decir, la representación de un hecho[1].

La noción más amplia de documento dentro del ámbito jurídico, es aquella que entiende por tal, que los objetos que tengan una función probatoria con la sola limitación de que dichos objetos, sean por su índole, susceptibles de ser llevados ante la presencia judicial[2].

Según el Diccionario Enciclopédico Universal, es el escrito con que se prueba o acredita una cosa.

El Diccionario Jurídico Elemental de Cabanellas, dice que el documento es: *“Instrumento, escritura, escrito con que se prueba, confirma o justifica alguna cosa o al menos, que se aduce con tal propósito. En la acepción más amplia, cuando consta por escrito gráficamente; así lo es tanto un testamento, un contrato firmado, un libro una carta, como una fotografía o un plano; y sea cualquiera la materia sobre la cual se extienda configure, aunque indudablemente predomine el papel sobre todas las demás. Cualquier comprobante o cosa que sirva para ilustrar. Diploma, inscripción, relato y todo escrito que atestigüe sobre un hecho histórico”*. Al conceptualizar la prueba

[1] KORNEGAY Ortez Eduardo y otros, “VALOR PROBATORIO”, Técnico Monerrey, compilado por Tellez Julio.

[2] KORNEGAY Ortez Eduardo y otros, “VALOR PROBATORIO”, Técnico Monerrey, compilado por Tellez Julio.

documental Cabanellas dice: *"la que se realiza por medio de documentos privados, documentos públicos, libro de comerciantes, correspondencia o cualquier otro escrito".*

Entendemos por documento cualquier *"objeto que contenga un información que narra, hace conocer o representa un hecho, cualquiera sea su naturaleza, su proceso de elaboración o su tipo de firma. De esto podemos desprender que se considera documento cualquier escrito, impreso, plano, dibujo, cuadro, fotografía, cintas cinematográficas, discos, grabaciones, magnetofónicas, radiográficas y en general todo objeto mueble que contenga carácter representativo declarativo."*[3]

*"Un instrumento, normalmente escrito, en cuyos textos se consiguen alguna cosa, apta para esclarecer un hecho o se deja constancia de una manifestación de voluntad que produce efectos jurídicos"*[4]

En la doctrina jurídica se podían diferenciar dos tendencias básicas al tratar de explicar la realidad documental jurídica y son[5]:

La Teoría del Escrito: requiere esta forma de expresión, se clasifican en públicos y privados.

La Teoría de la Representación: para la cual el documento no sólo es un escrito sino todo objeto representativo o que puede informar sobre un hecho o sobre otros objetos, (documentos técnicos materiales: fotografías, registros dactiloscópicos, documentos electrónicos, etc.)

---

[3] DELGADO Flores Gaudencio, TELLEZ Valdés Julio: "Temas de Derecho Informático". Primera Edición, Junio de 2006, Pág. 115 y 116.

[4] Fernandez del Pech, Horacio, "Internet: Su Problemática Jurídica" Editorial Abeledo - Perrot, sin año, Buenos Aires, pág. 251.

[5] ROMERO Olea, José Alfredo y REZA Valdespino Alfonso; "Los Documentos Electrónicos en el Derecho Procesal" UNAM, México.

El cambio de noción del documento escrito tradicional al documento electrónico, a hecho que la conceptualización del segundo vaya más allá de la vinculación al papel que es la forma de soporte o materialización de la información que contiene y que eran al igual que otros, los únicos conocidos y aceptado hasta hace poco. El documento electrónico pone de manifiesto la importancia que tiene la forma de su creación y los medios técnicos utilizados para su almacenamiento, transmisión y conservación.[6]

Las formas de representación de la información en medios electrónicos han hecho que los documentos sean de distintas formas: gráficos, de audio, video, alfanuméricos, etc., los cuales necesitan para su representación distintos tipos de tecnologías, pantallas, parlantes, impresoras, etc.; para su transmisión de redes de computadoras, telefonía móvil, fibras digitales, satélites, y para su conservación de distintas tecnologías como son: soportes magnéticos, electrónicos, digitales, ópticos, etc.[7] No todo documento en el que interviene el computador es electrónico, lo que requiere para que sea electrónico es esta forma de representación.

La desmaterialización de los documentos implica muchas ventajas, tanto en la transferencia de documentos rápida, fluida y compresible, sin errores, con reducción de recursos. Esta desmaterialización de la información en la que ya no se requiere únicamente de un soporte en papel, hace que nos replanteemos sobre la forma de valoración de la prueba documental.[8]

Tradicionalmente, el concepto de documentos ha venido identificando como “escrito”; es decir, como un objeto instrumento, en él que queda plasmado un hecho que se exterioriza mediante signos materiales y

[6] Valor Probatorio de los Documentos Electrónicos, apuntes del Dr. Julio Tellez Valdés, agosto del 2007.

[7] Valor Probatorio de los Documentos Electrónicos, apuntes del Dr. Julio Tellez Valdés, agosto del 2007.

[8] Valor Probatorio de los Documentos Electrónicos, apuntes del Dr. Julio Tellez Valdés, agosto del 2007.

permanentes de lenguaje. Sin embargo, acogiendo una definición amplia del documento, se lo entiende como cosas muebles aptas para la incorporación de señales expresivas de un determinado significado"[9] debemos concluir en que los registros o soportes electrónicos constituyen verdaderos documentos, pues en ellos se recogen expresiones del pensamiento humano de un hecho, incorporandolos a su contenido, que es lo que los hace capaces de acreditar la realidad de determinados hechos;[10] sin embargo, ya no podría considerase como un bien mueble, sino como un derecho.

La conceptualización de los documentos electrónicos y el establecer sus elementos, es complicado ya que la doctrina no encuentra unanimidad, a continuación se expone lo que manifiestan al respecto:

Carrara Valentín dice: *"Se caracteriza por el hecho de no poder ser leído por el hombre sin la utilización de la adecuada máquina que hagan perceptibles y compresibles las señales digitalesl de que están formados; y documentos electrónicos en sentido amplio son aquellos que pueden ser leídos por el ser humano de una forma directa, sin necesidad de utilizar una máquina traductora, pudiendo no obstante tener diversos modos de formación"*[11].

**Lorenzeytti** manifiesta que se trata de una declaración que está asentada sobre bits y no sobre átomos.[12]

---

[9] Cita de Caroca Pérez Alex, Ob. Cit. P. 294, en el documento de González Hernández, Horacio, "Valor Probatorio del Documento Electrónico", www.monografías.com/trabajos16/documento-electronico.zip

[10] González Hernández, Horacio, "Valor Probatorio del Documento Electrónico", www.monografías.com/trabajos16/documento-electronico.zip

[11] "El documento electrónico: Aspectos procesales" Revista Chilena de Derecho Informático. N° 4, mayo de 2004 Pág. 81-106. http://www.derechoinformatico.uchile.cl

[12] "El documento electrónico: Aspectos procesales" Revista Chilena de Derecho Informático. N° 4, mayo de 2004 Pág. 81-106. http://www.derechoinformatico.uchile.cl

Andrea SARRA expresa que el término electrónico hace referencia al dispositivo en el que está almacenado el instrumento o por medio del cual fue confeccionado.[13]

Para LEIVA Juan, el *"documento electrónico debe entenderse como toda expresión en lenguaje natural o convencional y cualquier otra expresión gráfica, sonora o en imágenes, recogidas en cualquier tipo de soporte material, incluso los soportes informáticos, con eficacia probatoria o cualquier otro tipo de relevancia jurídica".*[14]

Para la legislación chilena es *"toda representación informática que da testimonio de un hecho"*[15]

"Es la información inmaterializada o desmaterializada, concreta, visible y perceptible, por intermedio de un soporte material.[16]

*"Es el soporte o medio donde queda constancia de los datos, del proceso del resultado o de las decisiones que un sistema electrónico, informático telemático de cualquier tipo."*[17]

*"Toda información inteligible en formato electrónico o similar que puede ser almacenada o intercambiar por cualquier medio"*

---

[13] Valor Probatorio de los Documentos Electrónicos, apuntes del Dr. Julio Tellez Valdés, agosto del 2007.

[14] LEIVA, Juan, "Documentos Electrónicos" www.monografias.com/trabajos17/delec/delec.zip.

[15] LEIVA, Juan, "Documentos Electrónicos" www.monografias.com/trabajos17/delec/delec.zip.

[16] RIOS Estavillo, Juan José, " derecho e informática en México: informática jurídica y derecho a la informática" universidad nacional autónoma de México, 1997, pág. 134, www.juridicas.unam.mex/inst/direc/datper.htm?p=rios

[17] Davara Miguel Ángel, Citado por BARRIUSO Ruiz, Carlos "Interacción del Documento y la informática"

Entre estos conceptos existen elementos en común:

1. Información desmaterializada o inmaterializada.
2. Soporte Electrónico
3. La necesidad de un sopote material que permita hacer perceptible la información.

Para nuestra legislación el documento electrónico es un mensaje de datos, como lo establece la definición que realiza en la Disposición General Novena de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos; es decir, es toda información creada, generada, comunicada, enviada, recibida o procesada por cualquier medio electrónico y que puede ser intercambiada por cualquier medio. En estricto sentido sería entonces el documento electrónico el que está en formato electrónico, una información electrónica o digital que se ha creado, generado, recibido, comunicado, enviado, recibido o procesado por cualquier medio[18].

La doctrina hace una distinción asimismo sobre el documento jurídico en general y se dice que es aquello que puede tener alguna significación legal o procesal como cartas fotos, grabaciones, etc. Instrumento jurídico, en cambio, es únicamente el documento escrito a mano, o por medios mecánicos, electrónicos, pero realizado en todo caso con intervención de una persona, con la finalidad de perpetuar un hecho o un derecho cualquiera, dejando constancia del mismo, una carta, un recibo, un contrato en el cual una persona reconocer que debe una determinada cantidad de dinero a su acreedor por haberse efectuado una transacción. Resulta claro que la característica esencial que distingue el instrumento jurídico del documento, es el de ser realizado por escrito, y constar no sólo en un papel, ya que los documentos en general pueden contener otras formas de expresión como ocurre en la actualidad en los discos CDs, memorias flash, tarjetas de memorias, discos duros, etc. El Profesor Walter Guerrero distingue que el documento jurídico es el género y el

[18] BARZALLO Sacoto, José Luís, Apuntes de Clase Maestría de Derecho Informático, Universidad de Cuenca, 2007.

instrumento jurídico una de sus especies. Ya en el tema penal los documentos jurídicos pueden ser objeto de prueba como también medio de prueba[19].

Los requisitos que debe tener un instrumento jurídico son[20]:

**Sujeto otorgante**, el documento debe ser elaborado o conferido por una persona natural a jurídica a favor o en contra de la cual pueden presentar el instrumento, aunque también puede ser utilizado a favor o en contra de terceros. Se exige que el documento sea firmado por una persona que asume responsabilidad por su existencia o contenido.

**Materialización escrita:** debe ser elaborado por escrito, carecen de importancia los documentos adjuntos anexos, gráficos, planos o fotos.

**Tenor lógico:** se refiere a su contenido, requiere la existencia de un hecho o la declaración de un derecho, con contenido lógico y entendible.

**Autenticación:** Consiste en la necesidad de que en el instrumento conste el medio para acreditar o verificar que fue realmente otorgado por la persona a la que se atribuye, lo cual se hace por la firma, también se puede incluir sellos, timbres, distintivos, rúbricas, etc. En los instrumentos públicos, firma el competente empleado con las solemnidades establecidas, y en los instrumentos privados su autenticación se realiza con firmas y rúbricas de los otorgantes, con la impresión de la huella digital y en presencia de testigos si no pudieran o no supieran firmar. Si no tienen autenticación expresa pueden servir como medios de prueba tales como los libros de contabilidad, las tarjetas de entrada y salida del personal, talonarios de cheques, los mensajes de correo,

[19] VACA Andrade, Ricardo, "Manual de Derecho Procesal Penal" Tomo II , Cuarta edición, Corporación de Estudios y Publicaciones, 2009, Pág. 1047.

[20] VACA Andrade, Ricardo, "Manual de Derecho Procesal Penal" Tomo II , Cuarta edición, Corporación de Estudios y Publicaciones, 2009. Pág. 1048.

cuya autoría se puede establecer por medios técnicos, científicos, instrumentos todos estos que pueden autenticar mediante actuación pericial[21].

### 1.1.1 LA REGULACIÓN DEL DOCUMENTO ELECTRÓNICO EN LA LEGISLACIÓN ECUATORIANA

La existencia y utilización del documento electrónico entre los ecuatorianos y en distintos tipos de relaciones comerciales y sociales, generó la necesidad de su regulación, por lo que se dictó la Ley de Comercio Electrónico, Firmas Electrónicas Y Mensajes De Datos, mediante la Ley número 67, publicada en Registro Oficial Suplemento 557, de 17 de abril de 2002.

En esta ley se regulan algunos aspectos, entre ellos se dota de reconocimiento legal a los mensajes de datos, los cuales resultan ser el género y los documentos electrónicos solamente se convierten en especies, se regulan también las firmas electrónicas, entidades de certificación, servicios electrónicos, derechos de usuarios o consumidores, los Instrumentos Públicos, la prueba y notificaciones electrónicas, y se incluyen varias reformas al Código Penal, tipificando algunas infracciones informáticas.

Sobre los mensajes de datos y por ende los documentos electrónicos, el Art. 2 de la Ley de Comercio Electrónico, dispone que, para que tenga eficacia, sea valorado y produzca efectos el documento electrónico, debe cumplir los requisitos que establece la ley.

Esta misma norma legal determina los requisitos que debe contener los mensajes de datos, y por ende también los documentos electrónicos y siendo los siguientes:

[21] VACA Andrade, Ricardo, “Manual de Derecho Procesal Penal” Tomo II , Cuarta edición, Corporación de Estudios y Publicaciones, 2009, Pág. 1048

- **Accesibilidad**, es decir se puede recuperar su contenido en forma íntegra en cualquier momento empleando mecanismos y procedimientos previstos para el efecto.

- **Conservación** en formato original y que sea susceptible de determinar los datos de origen, destino, fecha y hora de creación, generación, procesamiento, envío, recepción y archivo. Lo cual se realiza con la firma electrónica y su certificado, o en su defecto con registros de otros tiempos de firma o sistemas de identificación o autenticación, tal como sellado de tiempo, sistemas biométricos, encriptación, etc.

- **Integridad,** lo cual implica que esté completo e inalterable y según el artículo seis del Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, se produce sí está firmado electrónicamente. Por lo tanto, para que el documento electrónico constituya un medio de prueba, se requiere que el mismo esté firmado electrónicamente, en caso que no tenga la firma electrónica, pasa a ser un indicio que necesariamente debe estar acompañado de otros medios de prueba, para que pueda producir efectos y ser tomado en cuenta por el Tribunal de Garantías Penal al momento de la valoración del mismo.

Existen algunos principios que están regulados en esta ley, y resultan importantes dentro de la presente investigación para determinar el alcance de los mismos, ya que rigen al documento electrónico y establecen sus requisitos legales para la validez, siendo los siguientes:

**PRINCIPIOS DE CONFIDENCIALIDAD Y RESERVA**.

Los mismos que están regulados en el Art. 5 de la Ley de Comercio Electrónico. La confidencialidad está relacionada con el secreto de comunicaciones privadas e implica una garantía entre las partes. Los documentos electrónicos se pueden asegurar con una firma electrónica de

clave pública y privada o formas de encriptación, tanto del mensaje (criptografía simétrica o asimétrica) como del canal con sistemas SSL o SET.

**PRINCIPIO DE NO REPUDIO O NON REPUDIATION:**

Es un principio con origen anglosajón, que permite a una persona que tiene en su poder el documento electrónico, probar que realmente ha sido otorgado y comunicado, protegiéndole ante una posible negación de existencia.

**PRINCIPIO DE AUTENTICIDAD**

Tiene relación con la integridad; es decir, que el documento es emitido por quien es su autor y en la forma que se presenta. Se relaciona con las Entidades de Certificación, porque ellas dan fe de que quien suscribe con una firma electrónica es la persona que dice ser.

**PRINCIPIO DE EQUIVALENCIA FUNCIONAL ENTRE LOS MENSAJE DE DATOS Y LOS DOCUMENTOS ESCRITOS.**

Principio que dota al documento electrónico de igual valor que los documentos escritos; este principio es uno de los más importantes en el tema ,ya que asimila y da validez legal tal como que se tratara de documentos escritos, es el eslabón entre el concepto tradicional de documento escrito y documento electrónico.

**PRINCIPIO DE ACCESIBILIDAD PARA SU POSTERIOR CONSULTA**

Los documentos electrónicos adolecen de escasa corporalidad y alta volatilidad, porque pueden modificarse o eliminarse fácilmente, y es lo que precisamente hace desconfiar de este tipo de documentos. A este principio también se le denomina de reproducción y está relacionado con la autenticidad y la integridad. Se regula este principio en el Art. 6 de la Ley de Comercio Electrónico. Por su parte el Art. 2 del Reglamento a la Ley de

Comercio Electrónico dispone: "***Art. 2.- Accesibilidad de la información***.- *Se considerará que un mensaje de datos, sus anexos y remitidos, son accesibles para consulta posterior cuando se puede recuperar su contenido en forma íntegra en cualquier momento empleando los mecanismos y procedimientos previstos para el efecto, los cuales deberán detallarse y proporcionarse independientemente del mensaje de datos a fin de garantizar el posterior acceso al mismo.*

***Art. 3***.- ***Información escrita***.- *Se entiende que la información contenida en un mensaje de datos es accesible para su posterior consulta cuando:*

*a) Ha sido generada y puede ser almacenada en un lenguaje electrónico/informático y formato entendibles por las partes involucradas en el intercambio de información y sus respectivos sistemas informáticos de procesamiento de la información, pudiéndose recuperar su contenido y el de los remitidos o anexos correspondientes en cualquier momento empleando los mecanismos previstos y reconocidos para el efecto; y,*

*b) Se puede recuperar o se puede acceder a la información empleando los mecanismos previstos al momento de recibirlo y almacenarlo, y que deberán detallarse y proporcionarse independientemente del mensaje de datos a fin de garantizar el posterior acceso al mismo.*

*Las publicaciones que las leyes exijan por escrito, sin perjuicio de lo establecido en dichas leyes, podrán adicionalmente efectuarse en medios electrónicos en forma de mensajes de datos.*

*Cumplidos los requisitos de accesibilidad, el mensaje de datos tiene iguales efectos jurídicos que los documentos que constan por escrito."*

**PRINCIPIO DE INCORPORACIÓN POR REMISIÓN**

Protege a los mensajes de datos, y todo lo que esté adjunto por remisión o anexo mediante un enlace directo, o sea, aceptado y conocido por las partes. (Adjuntos o atachados). Los hipervínculos deben ser directos y su aceptación debe ser expresa.

La aceptación que hacen las partes del contenido por remisión deberá ser expresada a través de un mensaje de datos que determine inequívocamente tal aceptación. En el caso de contenidos incorporados por remisión a través de un enlace electrónico, no podrá ser dinámico ni variable y por tanto la aceptación expresa de las partes se refiere exclusivamente al contenido accesible a través del enlace electrónico al momento de recepción del mensaje de datos.

En las relaciones con consumidores, es responsabilidad del proveedor asegurar la disponibilidad de los documentos remitidos o anexos para que sean accedidos por un medio aceptable para el consumidor cuando éste lo requiera. En las relaciones de otro tipo las partes podrán acordar la forma y accesibilidad de los anexos y remitidos.

Los anexos o remisiones referidos a garantías, derechos, obligaciones o información al consumidor deberán observar lo establecido en la Ley Orgánica de Defensa del Consumidor y su reglamento.

Toda modificación a un documento anexo o remitido, en un mensaje de datos se debe comunicar al receptor del mismo, a través de un mensaje de datos o por escrito, resaltando las diferencias entre el texto original y el modificado. En el texto modificado se deberá incluir en lugar visible y claramente accesible un enlace al contenido anterior. La comunicación al consumidor respecto de modificaciones no constituye indicación de aceptación de las mismas por su parte. Dicha aceptación deberá ser expresa y remitida por cualquier medio, ya sea éste físico o electrónico.

Cuando las leyes así lo determinen, cierto tipo de información deberá estar directamente incluida en el mensaje de datos y no como anexo o remitido.

**PROPIEDAD INTELECTUAL**

Los mensajes de datos se someten a las leyes de propiedad intelectual, según lo dispuesto en el Art. 4 de la Ley de Comercio Electrónico.

## INFORMACIÓN ORIGINAL

El Art. 7, de la Ley de Comercio Electrónico manifiesta: *"Información original.- Cuando la Ley requiera u obligue que la información sea presentada o conservada en su forma original, este requisito quedará cumplido con un mensaje de datos, si siendo requerido conforme a la Ley, puede comprobarse que ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos.*

*Se considera que un mensaje de datos permanece íntegro, si se mantiene completo e inalterable su contenido, salvo algún cambio de forma, propio del proceso de comunicación, archivo o presentación.*

*Por acuerdo de las partes y cumpliendo con todas las obligaciones previstas en esta Ley, se podrán desmaterializar los documentos que por ley deban ser instrumentados físicamente.*

*Los documentos desmaterializados deberán contener las firmas electrónicas correspondientes debidamente certificadas ante una de las entidades autorizadas según lo dispuesto en el artículo 29 de la presente ley, y deberán ser conservados conforme a lo establecido en el artículo siguiente."*

El Art. 4 del Reglamento a la Ley dispone: ***"Información original y copias certificadas.-*** *Los mensajes de datos y los documentos desmaterializados, cuando las leyes así lo determinen y de acuerdo al caso, deberán ser certificados ante un Notario, autoridad competente o persona autorizada a través de la respectiva firma electrónica, mecanismo o procedimiento autorizado.*

*Los documentos desmaterializados se considerarán, para todos los efectos, copia idéntica del documento físico a partir del cual se generaron y deberán contener adicionalmente la indicación de que son desmaterializados o copia electrónica de un documento físico. Se emplearán y tendrán los*

*mismos efectos que las copias impresas certificadas por autoridad competente."*

**PRINCIPIO DE ORIGINALIDAD**

"Que resulta de la inventiva de su autor". El problema es que el original de un documento digital está en el computador que se digitó, por ello es complementario el principio de integridad, ya que la ley no podrá exigir originales como en la forma tradicional, sino mas bien su integridad, por ello considero que requiere modificaciones el Código de Procedimiento Civil que solo admite como prueba los documentos originales. Sin embargo, si el documento requiere ser desmaterializado en ese caso esta regulado de la siguiente forma por el Reglamento a la Ley de Comercio Electrónico: "***Art. 5***.- *Desmaterialización.- El acuerdo expreso para desmaterializar documentos deberá constar en un documento físico o electrónico con las firmas de las partes aceptando tal desmaterialización y confirmando que el documento original y el documento desmaterializado son idénticos. En caso que las partes lo acuerden o la ley lo exija, las partes acudirán ante Notario o autoridad competente para que certifique electrónicamente que el documento desmaterializado corresponde al documento original que se acuerda desmaterializar. Esta certificación electrónica se la realiza a través de la respectiva firma electrónica del Notario o autoridad competente.*

*Los documentos desmaterializados deberán señalar que se trata de la desmaterialización del documento original. Este señalamiento se constituye en la única diferencia que el documento desmaterializado tendrá con el documento original.*

*En el caso de documentos que contengan obligaciones, se entiende que tanto el documento original como el desmaterializado son la expresión de un mismo acuerdo de las partes intervinientes y por tanto no existe duplicación de obligaciones. De existir multiplicidad de documentos desmaterializados y originales con la misma información u obligación, se entenderá que se trata del mismo, salvo prueba en contrario.*

*La desmaterialización de los documentos de identificación personal estará sujeta a las disposiciones especiales y procedimiento que las entidades competentes determinen.*

## CONSERVACIÓN DE MENSAJES DE DATOS

La información sometida a la Ley de Comercio Electrónico, podrá ser conservada; éste requisito quedará cumplido mediante el archivo del mensaje de datos, siempre que se reúnan las condiciones dispuestas en la Ley de Comercio Electrónico:

a. Que la información que contenga sea accesible para su posterior consulta;

b. Que sea conservado con el formato en el que se haya generado, enviado o recibido, o con algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida;

c. Que se conserve todo dato que permita determinar el origen, el destino del mensaje, la fecha y hora en que fue creado, generado, procesado, enviado, recibido y archivado; y,

d. Que se garantice su integridad por el tiempo que se establezca en el reglamento a esta ley.

Toda persona podrá cumplir con la conservación de mensajes de datos, usando los servicios de terceros, siempre que se cumplan las condiciones mencionadas en este artículo.

La información que tenga por única finalidad facilitar el envío o recepción del mensaje de datos, no será obligatorio el cumplimiento de lo establecido en los literales anteriores.

El Art. 9 del Reglamento a la Ley regula los requisitos que debe tener los servicios de conservación de mensajes de datos por terceros.

## PRINCIPIO DE INTEGRIDAD

Requisito que se plasma en el documento en donde consta toda la información que existía al momento de su emisión y que desde entonces no ha sido alterada.

Este requisito se cumple si el documento esta firmado electrónicamente, si no lo está será necesario probar al juez, que el documento no fue alterado, lo que se puede realizar de forma técnica.

El Art. 6 del Reglamento a la ley, dispone lo que debe entenderse por este requisito ***"Integridad de un mensaje de datos.-*** *La consideración de integridad de un mensaje de datos, establecida en el inciso segundo del artículo 7 de la Ley 67, se cumple si dicho mensaje de datos está firmado electrónicamente. El encabezado o la información adicional en un mensaje de datos que contenga exclusivamente información técnica relativa al envío o recepción del mensaje de datos, y que no altere en forma alguna su contenido, no constituye parte sustancial de la información.*

*Para efectos del presente artículo, se considerará que la información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún cambio que sea inherente al proceso de comunicación, archivo o presentación."*

El Art. 10 de la Ley establece la forma y las presunciones sobre la procedencia e identidad de la persona que remite un mensaje de datos: "*Art. 10.- Procedencia e identidad de un mensaje de datos.- Salvo prueba en contrario se entenderá que un mensaje de datos proviene de quien lo envía y, autoriza a quien lo recibe, para actuar conforme al contenido del mismo, cuando de su verificación exista concordancia entre la identificación del emisor y su firma electrónica, excepto en los siguientes casos:*

*a) Si se hubiere dado aviso que el mensaje de datos no proviene de quien consta como emisor; en este caso, el aviso se lo hará antes de que la persona que lo recibe actúe conforme a dicho mensaje. En caso contrario, quien conste como emisor deberá justificar plenamente que el mensaje de datos no se inició por orden suya o que el mismo fue alterado; y,*

*b) Si el destinatario no hubiere efectuado diligentemente las verificaciones correspondientes o hizo caso omiso de su resultado."*

El Art. 7 del Reglamento determina la forma de determinar la identidad del emisor de un mensaje de datos.

***Art. 7.- Procedencia e identidad de un mensaje de datos.-*** *La verificación de la concordancia entre el emisor del mensaje de datos y su firma electrónica se realizará comprobando la vigencia y los datos del certificado de firma electrónica que la respalda. En otros tipos de firmas o sistemas de identificación y autenticación, esta verificación se realizará mediante la verificación de los registros acordados o requeridos.*

*El aviso de un posible riesgo sobre la vulnerabilidad o inseguridad de una firma, su certificado o el mensaje de datos y los anexos relacionados podrá ser realizado por el titular de los mismos, mediante cualquier tipo de advertencia que permita, de manera inequívoca a quien realiza la verificación o recibe un mensaje de datos, tomar las precauciones necesarias para evitar perjuicios y prevenir fallas de seguridad. Este aviso deberá ser realizado antes de iniciar cualquier proceso de transacción comercial negociación, o contratación electrónica.*

*De acuerdo a las leyes, se podrá recurrir a peritos para determinar la procedencia y otro tipo de relaciones de un mensaje de datos con quien lo remite de modo directo o indirecto.*

**MOMENTO DE ENVÍO Y RECEPCIÓN DE MENSAJES DE DATOS.**

El Art. 11 de la Ley de Comercio Electrónico establece los momentos de emisión, recepción y el lugar de donde se realiza lo cual nos ayuda con respecto a las competencias jurisdiccionales judiciales.

*"Art. 11.- Envío y recepción de los mensajes de datos.- Salvo pacto en contrario, se presumirá que el tiempo y lugar de emisión y recepción del mensaje de datos, son los siguientes:*

*a) Momento de emisión del mensaje de datos.- Cuando el mensaje de datos ingrese en un sistema de información o red electrónica que no esté bajo control del emisor o de la persona que envió el mensaje en nombre de éste o del dispositivo electrónico autorizado para el efecto;*

*b) Momento de recepción del mensaje de datos.- Cuando el mensaje de datos ingrese al sistema de información o red electrónica señalado por el destinatario. Si el destinatario designa otro sistema de información o red electrónica, el momento de recepción se presumirá aquel en que se produzca la recuperación del mensaje de datos. De no haberse señalado un lugar preciso de recepción, se entenderá que ésta ocurre cuando el mensaje de datos ingresa a un sistema de información o red electrónica del destinatario, independientemente de haberse recuperado o no el mensaje de datos; y,*

*c) Lugares de envío y recepción.- Los acordados por las partes, sus domicilios legales o los que consten en el certificado de firma electrónica, del emisor y del destinatario. Si no se los pudiere establecer por estos medios, se tendrán por tales, el lugar de trabajo, o donde desarrollen el giro principal de sus actividades o la actividad relacionada con el mensaje de el datos.*

*El tiempo y lugar de envío se presumen, pero el hecho del envío no, pero cuando hay sellado de tiempo se establece la fecha y hora que el mensaje fue recibido por la certificador y recibido por el destinatario".*

### 1.1.2 LOS DOCUMENTOS ELECTRÓNICOS COMO MEDIOS DE PRUEBA

El Art. 53 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, establece la presunción sobre su validez.

Así, mismo el Art. 54 de la mencionada ley, ordena que en aquel documento electrónico, o sea un medio de prueba, será necesario que esté en soporte material (informático) sea trascrito en papel (impreso) y además es necesario proporcionar los elementos materiales electrónicos o informáticos necesarios para su lectura y verificación.

*"Práctica de la prueba.- La prueba se practicará de conformidad con lo previsto en el Código de Procedimiento Civil y observando las normas siguientes:*

*a) Al presentar un mensaje de datos dentro de un proceso judicial en los juzgados o tribunales del país, se deberá adjuntar el soporte informático y la transcripción en papel del documento electrónico, así como los elementos necesarios para su lectura y verificación, cuando sean requeridos;*

*b) En el caso de impugnación del certificado o de la firma electrónica por cualesquiera de las partes, el juez o tribunal, a petición de parte, ordenará a la entidad de certificación de información correspondiente, remitir a ese despacho los certificados de firma electrónica y documentos en los que se basó la solicitud del firmante, debidamente certificados;*

*c) El faxcímile, será admitido como medio de prueba, siempre y cuando haya sido enviado y recibido como mensaje de datos, mantenga su integridad, se conserve y cumpla con las exigencias contempladas en esta ley.*

*En caso de que alguna de las partes niegue la validez de un mensaje de datos, deberá probar, conforme a la Ley, que éste adolece de uno o varios vicios que lo invalidan, o que el procedimiento de seguridad, incluyendo los datos de creación y los medios utilizados para verificar la firma, no puedan ser reconocidos técnicamente como seguros"*

*Cualquier duda sobre la validez podrá ser objeto de comprobación técnica"*

La impugnación a este tipo de documentos será en razón de que carezca de seguridades, como por vicios que lo invalidan, los mismos que deben ser probados por quien los alega; sin embargo, será necesario cuidar la integridad del mensaje, para lo cual se deberá contar con un sistema que proteja de cualquier alteración al mensaje original[22] y de esta forma

[22] Esto se puede hacer con un tecnología denomina función hash [resumen del mensaje], que es un software que utiliza métodos criptográficos fuertes de 160 o 128 bits. Es análogo a una "suma de control" [checksum] o a un código de control de errores CRC [Cyclic Redundancy Checksum, Suma de Control de Redundancia Cíclica], en el sentido que representa de modo compacto el mensaje y es usado para detectar cambios en el mismo. Esta función se pede aplicar con un software adicional o está incluido en las funciones de firma electrónica simétrica como es el PGP. Tomado de Guía del Usuario Versión Gratuita PGP for Personal Privacy Versión 5.5 de Network Associates, Inc. http://www.nai.com

manteniéndolo completo, salvo algún cambio de forma, propio del proceso de comunicación, archivo o presentación, requisito denominado de originalidad, establecido en el Art. 7 de la Ley mencionada. En este aspecto será más fácil si se trata de un documento suscrito con una firma electrónica o digital que posea un certificado emitido por la entidad correspondiente y esté protegido con un código hash que es un software que utiliza métodos criptográficos y es usado para detectar cambios en el mismo. En caso de no tener estos aspectos, será necesario solicitar conjuntamente la intervención de un perito informático y una inspección para comprobar su integridad y originalidad.

De igual forma es necesario cumplir con los requisitos para su conservación, detallados en el Art. 8 del mismo cuerpo legal, por lo que se volverá importante demostrar tanto el contenido del documento así como establecer el origen del mensaje, información que generalmente se establece en las cabeceras de los email, lo que podrá ser clarificado para el entendimiento del juez o autoridad de forma imparcial por parte de un perito entendido en el tema.

También se podrá acompañar de los datos del servidor de alojamiento o soporte electrónico

Otra de las dudas que puede sobrevenir, es en el caso de no acordar la publicación del correo electrónico, y al ser aportado como prueba documental para demostrar el ilícito, se incorpora al expediente que no es reservado, haciéndose público, y podría pensarse que esta conducta se enmarca dentro de lo tipificado en el Art. 199 del Código Penal *"El que hallándose en posesión de una correspondencia no destinada a la publicación, la hiciera publicar, o presentare en juicio sin orden judicial, aunque haya sido dirigida a el, será reprimido con multa de seis a treinta y un dólares de los Estados Unidos de Norte América, si el acto puede causar perjuicio a terceros; a no ser que se trate de correspondencia en que consten obligaciones a favor del tenedor de ella, caso en el que puede presentarse en juicio"*

En el caso de que una de las partes solicite su incorporación al expediente, el juez podrá aceptar su entrega pero mandará a que se tengan de forma reservada, en especial en los asuntos ajenos a los hechos que son objeto del proceso.

Es necesario solicitar la retención, apertura o examen para que sea ordenada por el Juez de Garantías Penales, para evitar un atentado contra el derecho constitucional de inviolabilidad de correspondencia virtual.

Igualmente en la toma de la prueba se debe utilizar programas que demuestren su no alteración, ya sea con la utilización de funciones hash[23], las mismas que ayudan a determinar si un archivo electrónico o un mensaje sufrió alteración, utilizando sistemas de encriptación avanzados u otras tecnologías que tengan un fin semejante.

En armonía con este punto, no debemos olvidarnos de solicitar la intervención de un perito calificado y acreditado para el análisis técnico y tecnológico del documento electrónico que ayude al juez a valorar en forma correcta la prueba, según lo dispuesto en el Art. 55 de la Ley de Comercio Electrónico *"Valoración de la prueba.- La prueba será valorada bajo los principios determinados en la ley y tomando en cuenta la seguridad y fiabilidad de los medios con los cuales se la envió, recibió, verificó, almacenó o comprobó si fuese el caso, sin perjuicio de que dicha valoración se efectué con el empleo de otros métodos que aconsejen la técnica y la tecnología. En todo*

[23] Esto se puede hacer con una tecnología denomina función hash [resumen del mensaje], software que utiliza métodos criptográficos fuertes de 160 o 128 bits. Es análogo a una "suma de control" [checksum] o a un código de control de errores CRC [Cyclic Redundancy Checksum, Suma de Control de Redundancia Cíclica], en el sentido que representa de modo compacto el mensaje y es usado para detectar cambios en el mismo. Esta función se pede aplicar con un software adicional o está incluido en las funciones de firma electrónica simétrica como es el PGP. Tomado de Guía del Usuario Versión Gratuita PGP for Personal Privacy Versión 5.5 de Network Associates, Inc. http://www.nai.com

*caso la valoración de la prueba se someterá al libre criterio judicial, según las circunstancias en que hayan sido producidas.*

*Para la valoración de las pruebas, el juez o árbitro competente que conozca el caso deberá designar los peritos que considere necesarios para el análisis y estudio técnico y tecnológico de las pruebas presentadas."*

Sin embargo, el Código de Procedimiento Civil, en el Art. 199 dispone lo siguiente: *"Las cartas dirigidas a terceros, o por terceros, aunque en ellas se mencione alguna obligación, no serán admitidas para su reconocimiento, ni servirán de prueba."* Esta disposición puede afectar la valoración de los correos electrónicos si son dirigidos o realizados por terceros. Por esta razón es necesario acudir a otros medios de pruebas.

Así mismo, es necesario tomar en cuenta las disposición establecida en el nuevo Código Orgánico de la Función Judicial: *"**Art. 147.- VALIDEZ Y EFICACIA DE LOS DOCUMENTOS ELECTRÓNICOS**.- Tendrán la validez y eficacia de un documento físico original los archivos de documentos, mensajes, imágenes, bancos de datos y toda aplicación almacenada o transmitida por medios electrónicos, informáticos, magnéticos, ópticos, telemáticos, satelitales o producidos por nuevas tecnologías, destinadas a la tramitación judicial, ya sea que contengan actos o resoluciones judiciales. Igualmente los reconocimientos de firmas en documentos o la identificación de nombre de usuario, contraseñas, claves, utilizados para acceder a redes informáticas. Todo lo cual, siempre que cumplan con los procedimientos establecidos en las leyes de la materia.*

*Las alteraciones que afecten la autenticidad o integridad de dichos soportes les harán perder el valor jurídico que se les otorga en el inciso anterior, sin perjuicio de la responsabilidad penal en caso de que constituyan infracción de esta clase.*

*Todas las disposiciones legales que, sobre la validez y eficacia en juicio de los documentos que se hallan contenidas en el Código Civil, Código de Procedimiento Civil, Código de Procedimiento Penal, Ley de la Jurisdicción*

*Contencioso Administrativa, Código Tributario y otros cuerpos legales, se interpretarán de conformidad con esta norma, salvo los casos de los actos y contratos en que la ley exige de la solemnidad del instrumento público, en que se estará a lo prevenido por el artículo 1718 del Código Civil.*

*Cuando una jueza o juez utilice los medios indicados en el primer párrafo de este artículo, para consignar sus actos o resoluciones, los medios de protección del sistema resultan suficientes para acreditar la autenticidad, aunque no se impriman en papel ni sean firmados, pero deberán ser agregados en soporte material al proceso o archivo por el actuario de la unidad.*

*Las autoridades judiciales podrán utilizar los medios referidos para comunicarse oficialmente entre sí, remitiéndose informes, comisiones y cualquier otra documentación.*

*El Consejo de la Judicatura dictará los reglamentos necesarios para normar el envío, recepción, trámite y almacenamiento de los citados medios; para garantizar su seguridad, autenticidad e integridad; así como para posibilitar el acceso del público a la información contenida en las bases de datos, conforme a la ley."*

## 1.1 Tipos de Documentos Electrónicos: Públicos y Privados.

Esta es la clasificación más común de los documentos en el derecho, y proviene de la forma que se utiliza para su creación. *"Los documentos pueden clasificarse en públicos y privados, siendo los últimos aquellos que para su creación no interviene ningún tipo de terceros, es decir es creado por su autor y no requiere de ningún tipo de certificación y ya sea porque lo requiere o simplemente porque no lo solicita, a diferencia de los documentos públicos en donde expresamente se solicita la intervención de un tercero, comúnmente denominado Notario Público que certifica y dan fe de la creación del documento o de la identidad de aquellas que intervienen en su elaboración, de esta manera el documento tiene la más alta clasificación de seguridad, integridad,*

*autenticidad y permanencia que el derecho le puede otorgar, en otras palabras, será actor del mayor valor probatorio posible"*.[24]

En nuestra legislación ecuatoriana, los Instrumentos públicos están definidos en la ley:

El Art. 164 del Código de Procedimiento Civil dice: "*Instrumento Público Auténtico es el autorizado con las solemnidades legales por un competente empleado. Si fuere otorgado ante un notario que incorporado en protocolo registro público se llama escritura pública.*

*Se concederán también instrumentos públicos los mensajes de datos otorgados, conferidos, autorizados o expedidos por y ante autoridad competente y firmados electrónicamente".*

El Art. 51 de la Ley de Comercio Electrónico dice: *"Instrumentos Públicos Electrónicos. Se reconocen la validez jurídica de los mensajes de datos otorgados, conferidos, autorizados o expedidos por y ante autoridad competente y firmados electrónicamente.*

*Dichos instrumentos públicos electrónicos deberán observar los requisitos, formalidades y solemnidades exigidos por la ley y demás normas aplicables."*

INSTRUMENTO PRIVADO: El Art. 191 del Código de Procedimiento Civil dice: *"el escrito hecho por personas particulares, sin intervención del notario ni de otra persona legalmente autorizada, o por personas públicas en actos que no son de su oficio".* Por lo tanto de acuerdo con la ley, el instrumento privado puede ser de distintas clases, el Art. 193, del Código Procedimiento Civil señala cuáles son: las cartas; las partidas de entrada y los gastos diario; los libros administrativos y los de caja; las cuentas extrajudiciales; los inventarios,

[24] DELGADO Flores Gaudencio, TELLEZ Valdés Julio: "Temas de Derecho Informático". Primera Edición, Junio de 2006, Pág. 115 y 116.

tasaciones, presupuestos extrajudiciales y asientos privados; y, los documentos que hablan los artículos 192, y 194, del Código Procedimiento Civil.

Existen otras clasificaciones que se hacen de los documentos, teniendo en cuenta otros criterios de clasificación, distintos a los sujetos, como es el que divide en documentos públicos y privados, así tenemos por su fin, por su función probatoria, como lo enseña el doctrinario Fenech.

**Nominativos o anónimos**; según se identifica a la persona que hace la declaración expresa o no.

**Auténticos o falsos**.- Es una derivación de la clasificación anterior, ya que el documento autentico está relacionado con la persona que aparece como autor, porque sus expresiones, afirmaciones, o negaciones las asume con responsabilidad, sino existe esta relación entre autor-contenido del documento es falso. La prueba documental tiene esta característica, que una vez establecida la autenticidad del documento queda probada que la declaración contenida fue prestada por el otorgante.

**Por el fin** los documentos pueden ser:

**Constitutivos o Instrumentales.-** Son los que desde su inicio fueron elaborados como medios de prueba inmediata o mediata, la primera como la declaración escrita del procesado, un informe médico; y el medio de prueba mediato; son aquellas que recogen por escrito un medio de prueba que fue originalmente distinto del documental documentos que forman parte de otros procesos.

Los **documentos de eventualidad**: Son los que no adquieren el valor probatorio al momento de su creación, ni por voluntad de su autor, sino lo adquieren en forma  sino posterior.

Se clasifican también por su **función probatoria** y pueden ser:

**Documentos narrativos:** son los que contienen un relato o que consiste en una afirmación de ciertos hechos o de la experiencia.

**Documentos constitutivos**; no necesariamente contienen afirmaciones o relatos acerca del acontecido, sino buscan determinar que el autor del documento, haya hecho la declaración contenida en él; por lo que se vuelve necesario probar la autenticidad del documento y de la declaración contenida en él.

## 1.2 ANÁLISIS DE ALGUNOS ARTÍCULOS DEL CAPÍTULO IV DE LA PRUEBA DOCUMENTAL DEL CÓDIGO DE PROCEDIMIENTO PENAL.

*"**Art. 148**.- Cuando el documento fuere impugando, la Fiscal o el Fiscal, la Jueza o el Juez podrá ordenar la prueba pericial, con intervención de especialistas de la Policía Judicial.*

***Art. 149**.- Informes.- Los fiscales, jueces de garantías penales y tribunales de garantías penales pueden requerir informes sobre datos que consten en registros, archivos, incluyendo los informáticos.*

*El incumplimiento de estos requerimientos, la falsedad del informe o el ocultamiento de datos, serán sancionados con una multa equivalente al cincuenta por ciento de un salario mínimo vital general, sin perjuicio de la responsabilidad panal, si el hecho constituye un delito.*

*Los informes se solicitarán por escrito, indicando el proceso en el cual se requieren, el nombre del procesado, el lugar donde debe ser entregado el informe, el plazo para su presentación y la prevención de las sanciones previstas en el inciso anterior.*

***Nota:** Artículo reformado por Ley No. 67, publicada en Registro Oficial Suplemento 555 de 24 de Marzo del 2009.*

***Art. 152***.- *Otros documentos.- Cuando la infracción o la culpabilidad del encausado se pudieren probar por documentos que no sean de los mencionados en el Art. 150, el Fiscal los examinará. No podrá hacerse este examen sino en presencia del procesado o de su defensor, si los hubiere, o, a falta de estos, ante dos testigos, quienes jurarán guardar reserva. Se redactará el acta de la diligencia, que deberá ser firmada por los concurrentes. Si los documentos contuvieren datos relacionados con la infracción, se los agregará al expediente, después de rubricados. En caso contrario, se los devolverá al interesado.*

***Art. 156***.- *Documentos semejantes.- El juez de garantías penales autorizará al Fiscal para el reconocimiento de las grabaciones mencionadas en el artículo anterior, así como de películas, registros informáticos, fotografías, discos u otros documentos semejantes. Para este efecto, con la intervención de dos peritos que jurarán guardar reserva, el Fiscal, en audiencia privada, procederá a la exhibición de la película o a escuchar el disco o la grabación y a examinar el contenido de los registros informáticos. Las partes podrán asistir con el mismo juramento.*

*No se requerirá la autorización a la que se refiere el artículo anterior, en los casos en que las grabaciones de audio o video sean obtenidas por cámaras de seguridad o en lugares públicos; así como tampoco en los casos en que se divulguen grabaciones de audio o video obtenidas por uno de los intervinientes. En estos casos el juez de garantías penales tendrá la facultad de admitir o no la prueba obtenida a través de estos medios, valorando su autenticidad, la forma en que se obtuvo, los derechos en conflicto, y el bien jurídico protegido.*

*El Fiscal podrá ordenar la identificación de voces grabadas por personas que afirmen poder reconocerlas, sin perjuicio de ordenar el reconocimiento por medios técnicos o con intervención pericial.*

*Si los predichos documentos tuvieren alguna relación con el objeto y sujetos del proceso, el Fiscal ordenará redactar la diligencia haciendo constar en ella la parte pertinente al proceso. Si no la tuvieren, se limitará a dejar*

*constancia, en el acta, de la celebración de la audiencia y ordenará la devolución de los documentos al interesado.*

***Nota:*** *Artículo reformado por Ley No. 101, publicada en Registro Oficial Suplemento 555 de 24 de Marzo del 2009.*

***Art. ...****.- Los Fiscales podrán utilizar todos aquellos medios técnicos, electrónicos, informáticos y telemáticos que resulten útiles e indispensables para sustentar sus actuaciones y pronunciamientos, cumpliendo con los requisitos y obteniendo las autorizaciones que se exijan en la ley respecto de la procedencia y eficacia de los actos de investigación o de prueba que se formulen a través de dichos medios.*

*Las actuaciones que se realicen, y los documentos o información obtenidas a través de estos procedimientos, serán válidos y eficaces siempre que se garantice su integridad, autenticidad y reproducción, y no afecten en modo alguno los derechos y garantías fundamentales reconocidas en la Constitución y la ley.*

*Las actuaciones y procesos que se tramiten con soporte informático, deberán garantizar la confidencialidad, privacidad y seguridad de los datos e informaciones de carácter personal que contengan.*

*Sin embargo, en aquellos casos de grabaciones o filmaciones relacionadas a un hecho constitutivo de infracción, registradas de modo espontáneo al momento mismo de su ejecución, por los medios de comunicación social o por cámaras de seguridad, ubicadas en lugares públicos, le servirán al fiscal para integrar la investigación y para introducirlas al juicio como elemento de prueba para su valoración. Estas no requerirán de la autorización a la que se refiere el artículo ciento cincuenta y cinco.*

***Nota:*** *Artículo agregado por Ley No. 101, publicada en Registro Oficial Suplemento 555 de 24 de Marzo del 2009."*[25]

Estos artículos regulan la prueba documental dentro de nuestro Código de Procedimiento Penal, los cuales se han visto modificados con la reforme de marzo del 2009, que buscó agregar aspectos de trascendencia que mejore el sistema acusatorio oral y acepten los medios de prueba electrónicos, principalmente en este capítulo.

Los documentos electrónicos y la prueba electrónica en general, se aceptan como una forma especial de prueba documental, esto debido a que los documentos tienen una forma escrita en la representación así sea inmaterial el soporte.

Por esta razón se trató de asimilar a prueba documental tradicionalmente regulada; esto es que si el documento electrónico es impugnado los Fiscales o Jueces deben ordenar la prueba pericial, para lo que se debe nombrar un perito de la Policía Judicial, norma que no es coherente nuevamente con el sistema acusatorio oral, esto es en donde la prueba solamente puede ser pedida y solicitada por las partes; en el caso del Fiscal puede ordenar en la etapa de la indagación previa o la instrucción fiscal, en donde tendrá indicios, los mismos que solamente al momento del juicio se convertirán en prueba al igual que la defensa. Sin embargo el Juez puede mandar a practicar esta prueba, sin embargo determinar el momento es lo complicado, ya que como manifesté el sistema acusatorio oral impide que el Juez pueda mandar a practicar una prueba, en virtud del "Dispositivo", en donde las partes pueden impulsar el proceso, mas no el Juez.

[25] Copia realizada del programa SILEC, de la empresa LEXIS, del Código de Procedimiento Penal del Ecuador, publicada en la Ley 0, Registro Oficial Suplemento 360, de fecha 13 de enero del 2000, con las reformas de marzo del 2009.

Es necesario manifestar que la prueba pericial dentro de los documentos electrónicos, es de vital importancia por la complejidad en la valoración de los mismos, ya que se requiere contar con elementos que aseguren su autenticidad, integridad y reproducción. Sin embargo, la limitación que se realiza al solamente poder recurrir a peritos de la policía judicial, hace que los resultados se vean ligados a los profesionales, las técnicas, y las tecnologías que se encuentren en poder de esta institución. Ante la carencia de técnicos de la policía, en la práctica se han acreditado peritos civiles y conocedores de las tecnologías, quienes poseen equipos limitados, pero que pueden ayudar de mejor forma al análisis de las evidencias electrónicas o informáticas.

El Art. 149 del Código Adjetivo Penal, permite que los Fiscales, Jueces y Miembros de Tribunal, puedan solicitar informes sobre datos que consten en registros o archivos informáticos, bajo la pena de una multa en caso de incumplimiento, falsedad u ocultamiento. La forma de emitir estos informes es por escrito, indicando el proceso, el nombre del procesado, el lugar donde se entrega el informe, el plazo de presentación y la prevención sobre las sanciones. Con esta norma, se puede acceder a datos que consten en documentos informáticos, los mismos que pueden ser remitidos por escrito, lo cual implica que debe enviarse el documento en forma de registro informático, así como su impreso.

Es necesario tener en consideración que los datos que puedan contener sean datos personales, en este caso es necesario saber que el Art. 66 de la Constitución consagra como derecho en la siguiente forma:

*11. El derecho a guardar reserva sobre sus convicciones. Nadie podrá ser obligado a declarar sobre las mismas. En ningún caso se podrá exigir o utilizar sin autorización del titular o de sus legítimos representantes, la información personal o de terceros sobre sus creencias religiosas, filiación o pensamiento político; ni sobre datos referentes a su salud y vida sexual, salvo por necesidades de atención médica.*

*19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.*

Por lo tanto no se puede autorizar la remisión de informes sobre datos referentes a filiación o pensamiento política, creencias religiosas, salud o vida sexual. Cuando se trate de otros datos de carácter personal, por mandato del artículo analizado es posible su difusión, y digo esto en virtud de que el expediente una vez que sale de la investigación, y se inicia el proceso penal con la instrucción fiscal, se convierte en público.

Respecto al Art. 156 del Código de Procedimiento Penal, hace referencia a los documentos electrónicos cuando dice registros informáticos y otros documentos semejantes, en los cuales es necesario contar con la autorización del Juez Penal para proceder al reconocimientos de los mismos en una audiencia privada para examinar los registros o documentos informáticos, diligencia en la que el Fiscal debe nombrar dos peritos, quienes jurarán mantener en reserva. Si los documentos reconocidos tienen relación con el objeto y los sujetos del proceso, se redactar en un acta la parte pertinente; si no ha relación solamente se sienta la constancia en el acta y se devuelven los originales.

En esta norma caben algunas reflexiones:

- Que sucedería si el registro informático posee gran cantidad de información y se convierte esta en una prueba decisiva para el proceso; en este caso será necesario imprimir la información relevante o capturar sus imágenes y pegar en el acta de reconocimiento, así mismo la intervención de los peritos no solo es para atestiguar sino para realizar un análisis de la misma, por lo que será necesario efectuar algunas pruebas que determinen la autenticidad, integridad, las seguridades, originalidad del documento y asuntos relacionados al mismos, por

ejemplo si es una página web, es necesario contar con los datos del servidor de alojamiento de información, las seguridades, cambios, protocolos usados, usuarios, IP, etc.

- Si se tratan de imágenes en video, la impresión de las capturas de alguna información relevante será importante, si tiene audio será necesario la trascripción de los sonidos y palabras. Aquí los peritos deberán determinar los formatos del video y/o audio con el fin de hacerlo reproducible, teniendo en cuenta las tecnologías necesarias para este fin, etc.

Sin embargo, de lo manifestado, si los registros, videos, grabaciones electrónicas son relevantes, es necesario realizar un peritaje completo, con el objeto de que la evidencia pueda sustentar una instrucción fiscal, y una acusación penal, o en el caso de la defensa sirva con este propósito, y pueda ser introducida en el juicio, no como prueba documental propiamente, sino sea acreditada con el testimonio de los peritos y de los testigos de ser posible, esto por el hecho que el procedimiento es oral antes que escrito en esta etapa, por lo que será mejor actuarla de esta forma antes que solamente por escrito.

El artículo innumerado agregado a continuación del Art. 156 del Código Procedimiento Penal, faculta a los Fiscales utilizar para sustentar sus actuaciones y pronunciamientos, todos los medios técnicos, electrónicos, telemáticos, informáticos. Para entenderlo el alcance de estas expresiones nos remitiremos al criterio de Dr. Efraín Torres Chaves[26] "la palabra **Electrónico** debemos entenderla como perteneciente o relativo a electrón, a la electrónica que es la ciencia que estudia dispositivos basados en el movimiento de los electrones libres en el vacío, gases, o semiconductores, cuando dichos electrones están sometidos a la acción de esos campos electromagnéticos". También a la palabra electrón se la entiende "como la técnica que aplica a la

[26] TORRES Chaves, Efraín, "Breves Comentarios a la Ley de Comercio Electrónico Firmas Electrónicas y Mensajes de Datos" editorial Corporación de Estudios y Publicaciones, Quito.

industria los resultados de esta ciencia". La palabra "**informático**" debemos entenderla como "el conjunto de conocimientos científicos y técnicos que hacen posible el tratamiento automático de la información por medio de ordenadores". Telemático, palabra que viene de dos raíces, tele del griego Tele = distancia, es decir un sistema de telecomunicaciones de la informática.

Los **medios electrónicos** se refieren a la técnica de aplicación a la industria de la ciencia de la electrónica; es decir, el estudio de los dispositivos basados en el movimiento de electrones libres en el vacío, gases o semiconductores, cuando dichos electrones están sometidos a la acción de campos electromagnéticos[27].

La norma ordena que estos medios sean obtenidos con las autorizaciones necesarias para la procedencia y eficacia de los actos de investigación o de prueba.

Sin embargo, en el primer inciso del artículo analizado también se solicita que cumpla con los requisitos que establece la ley, lo cual parece que produce un vació, el cual es aclarado en el segundo inciso al manifestar que las actuaciones y los documentos o información contenida es válida y eficaz, siempre que se garantice su integridad, autenticidad, reproducción y no se afecten los derechos y garantías fundamentales reconocidas en la Constitución y la ley.

Respecto a los requisitos de integridad, autenticidad y reproducción, serán analizados en el último capítulo del presente trabajo, y sobre los derechos y garantías fundamentales reconocidas en la Constitución y la ley, es un tema sumamente amplio, a pesar de ello parece importante mencionar algunos aspectos constitucionales y legales que pueden aclarar el sentido de esta norma.

---

[27] TORRES Chaves, Efraín, "Breves Comentarios a la Ley de Comercio Electrónico Firmas Electrónicas y Mensajes de Datos" editorial Corporación de Estudios y Publicaciones, Quito

Sobre los derechos fundamentales, se podrán referirse entre otros a los siguientes:

- **DERECHO DE INTIMIDAD**: La protección a la intimidad no solamente es de carácter particular, y familiar sino incluso cuenta con proyección social, ya que la inobservancia de este bien produciría graves perjuicios en este ámbito. Se considera que la protección a la intimidad resguarda un bien de gran importancia como es "la libertad humana", ya que esta no se pudiera desarrollar con la intromisión de otros sujetos sociales que coarten el ejercicio de éste derecho. A la intimidad se la ha definido por Webster "como el derecho a ser dejado solo, a ser preservado de cualquier inspección u observación no autorizada, de indagaciones acerca del sí mismo o de sus negocios". La Constitución de la República garantiza el Derecho a la Intimidad en el numeral 20 del artículo 66 de la siguiente manera: *"El derecho a intimidad personal y familiar." El artículo 12 de la Declaración Universal de los Derechos Humanos dispone: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataque a su honra o a su reputación, toda persona tiene derecho a la protección de la ley contra tales injerencias y ataques" Casi el mismo texto consta en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos y en La Convención Americana sobre Derechos Humanos del Pacto de San José de Costa Rica. La disposición novena de la Ley de Comercio Electrónico, explica que se debe entender por intimidad: "**Intimidad.-** El derecho a la intimidad previsto en la Constitución de la República, para efectos de esta Ley, comprende también el derecho a la privacidad, a la confidencialidad, a la reserva, al secreto sobre los datos proporcionados en cualquier relación con terceros, a la no divulgación de los datos personales y a no recibir información o mensajes no solicitados".*

- **DERECHO DE PROTECCIÓN DE DATOS**: La protección del derecho a la intimidad ha llevada a que las legislaciones velen por los datos que se puede obtener de una persona, en nuestro país se encuentra

contemplado en el numeral 19 del Art. 66 de la Constitución de la siguiente manera: *"El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley".* Así como definido en la disposición novena de la Ley de Comercio Electrónico, a través de los siguientes términos, aunque se restringa a este cuerpo normativo:

- ***Datos personales:*** *Son aquellos datos o información de carácter personal o íntimo, materia de protección en virtud de esta Ley.*

- ***Datos personales autorizados****: Son aquellos datos personales que el titular ha accedido a entregar o proporcionar de forma voluntaria, para ser usados por la persona, organismo o entidad de registro que los solicita, solamente para el fin para el cual fueron recolectados, el mismo que debe constar expresamente señalado y ser aceptado por dicho titular.*

A estos datos personales se los ha clasificado doctrinariamente en:

- **Datos personales públicos**.- Son aquellos que constan en registros, documentos, bases de datos de instituciones públicas del Estado, encargados generalmente en la identificación de los individuos. Se ha discutido mucho de los datos que existen sobre antecedentes penales, se consideran que son datos sensibles pues incumben sólo individuo y al Estado y no a los demás asociados, pero en el ámbito ecuatoriano estos datos son públicos y cualquier persona puede acceder a ellos. Igualmente los procesos judiciales son públicos como lo establece la Constitución, salvo las excepciones que establece la misma ley. Por tanto son datos públicos todos aquellos que conste en

documentos públicos y su exhibición o divulgación no esté prohibida por ley.

- **Datos personales íntimos.**- Que se dividen en:

  **a)** **Datos sensibles**.- Son los que revelan el origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referida a la vida sexual[28]. Según lo que dispone el inciso segundo del artículo 21 del Reglamento a la Ley Comercio Electrónico hemos de entender como datos sensibles del consumidor: *"Se consideran* ***datos sensibles del consumidor*** *sus datos personales, información financiera de cualquier tipo como números de tarjetas de crédito, o similares que involucren transferencias de dinero o datos a través de los cuales puedan cometerse fraudes o ilícitos que le afecten."*

  **b)** **Datos personales íntimos no sensibles**.- Son todos aquellos que pertenecen al ámbito privado del individuo ya sea familiar y personal, que no tenga la categoría de sensibles. Se los denomina también datos esenciales pues permiten identificar a la persona así por ejemplo el nombre, el apellido, la actividad laboral que desempeña, etc.

Con respecto a los datos sensibles podemos apreciar que están íntimamente relacionados con algunos Derechos Constitucionales, como los regulados en los Art. 66 numerales 4, 5, 6, 8, 9, 10, 11, 12, 18, 19 y 21, de la Constitución de la República.

---

Art. 2 de la Ley de Protección de datos personales 25.326 cita por FERNADEZ DELPECH, Horacio "Internet y su problemática jurídica" editorial Abeledo-Perrot. Buenos Aires.

**DERECHO DE INFORMACIÓN.-** La Constitución lo reconoce en los Art. 16, 17, 18, 19 y 20. La Ley Orgánica de Transparencia y Acceso a la Información Pública, publicada en el Registro Oficial suplemento Nº 337 del 18 de mayo de 2004 y su Reglamento dictado mediante Decreto Ejecutivo 2471, publicado en el registro Oficial Nº 507 del 19 de enero de 2005, garantiza el Derecho de Información por parte del Estado y su pertenencia al ciudadano, la publicidad en todas la instituciones del Estado y las de derecho privado que tengan finalidad social o cuenten con participación del Estado, la gratuidad en su acceso, su apertura, transparencia que permiten la participación ciudadana en la toma de decisiones de interés general y rendición de cuentas de las autoridades, así mismo establecen procedimientos administrativos y recursos judiciales de acceso a la información, ahora regulado por la Constitución y la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, así como el Recurso de Habeas Data.

- **DERECHO DE LIBERTAD DE EXPRESIÓN:** Entre una de la libertades fundamentales del ser humano tenemos la de expresar nuestras ideas, pensamientos, sentimientos para que sean oídos por personas determinadas; es decir, dentro de un círculo social, familiar, laboral que conozcamos, o dirigidas a un número indeterminado de personas. Este derecho de expresión puede verse limitado por otras restricciones legales, de ámbito constitucional, como son los derechos de otro ser humano a la honra, imagen, libertad, intimidad, patrimonio, etc., secretos comerciales o industriales, sigilo profesional, no competencia desleal. Con la aplicación jurisprudencial del principio de proporcionalidad, sustentado en la necesidad social imperiosa y proporcional al fin legitimo perseguido, se ha dejado de lado el principio de buena fe.

- **DERECHO DE INVIOLABILIDAD DE CORRESPONDENCIA:** La norma constitucional contenido en el numeral 21 del Art. 66 de la Constitución de la República, replantea el concepto tradicional de correspondencia, ya que incluye el concepto de correspondencia virtual, entendida esta,

como mensajes de datos electrónico de envió y recepción por medios telemáticos. Sin embargo, al final va más allá y protege con la inviolabilidad y secreto a cualquier forma de comunicación, es decir establece a las formas y tipos de comunicación como el género, siendo el correo tradicional y virtual solo una especie, lo cual es acertado ya que un principio constitucional no puede reducir los conceptos en tipos y formas solamente tradicionales y conocidas, sino debe ser abierto a las innovaciones en los medios de comunicación, en armonía con los tiempos en donde las tecnologías y principalmente las aplicadas en la comunicación tienden a fusionarse y avanzar vertiginosamente. El Art. 66 de la Constitución lo regula en la siguiente forma: *"21. El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación."* La **comunicación** como bien jurídico, es un término amplio ya que debe entenderse como cualquier medio apto para transmitir el pensamiento, o como para el Diccionario de la Real Academia de la Lengua Española, en su tercera acepción *"transmisión de señales mediante un código común al emisor y receptor*, *en donde claro que ese código común a más de signos, símbolos o claves previamente acordadas puede estar constituido por un idioma, lenguaje o dialecto"*[29]. Sin embargo cuando dice forma o tipo de comunicación lo hace muy extenso, ya que la comunicación no solo puede ser de información materializada o desmaterializada, sino también de cosas. El desarrollo constitucional europeo ha implementado estos nuevos conceptos a la protección de los derechos fundamentales, así por ejemplo *"La Sentencia del Tribunal Constitucional Español 70/2002, de fecha 3 de abril contiene una especial protección de las comunicaciones, cualquiera que sea el sistema empleado para realizar: "Ciertamente los avances tecnológicos que en los últimos tiempos se han producido en el ámbito de las*

[29] "El Secreto en el Derecho Penal Colombiano"

*telecomunicaciones, especialmente en conexión con el uso o del concepto de comunicación y del objeto de protección del derecho fundamental, que extiéndala protección a estos nuevos ámbitos"*[30]

Respecto a los derechos fundamentales, que protege la ley, resulta ser muy poco concreto, sin embargo, las mismas maneras de actuar con la prueba documental, ya sea esta correspondencia, forma de comunicación, llamadas telefónicas, y los mismos documentos electrónicos prevé necesariamente la autorización judicial, es por tanto el juez quien determinará si es procedente o no, valorando la necesidad del medio de prueba y los derechos de las partes. Así mismo es necesario anotar que los derechos fundamentales están consagrados en la Constitución y la misma también les de categoría de fundamentales a los establecidos en convenios internacionales; sin embargo, la especificidad de la Constitución actual hace difícil encontrar derechos reconocidos en Instrumentos Internacionales que no estén contemplados en nuestra carta fundamental y desarrollados en las leyes secundarias.

[30] ROING Batalla, Antoni; GALA Carolina, MARTÍNEZ Daniel y MUÑOZ José "El Uso laboral y Sindical del Correo Electrónico e Internet en la Empresa" Editado por Tirant lo Blanch, Valencia 2007, pág. 72.

# CAPITULO II

# LA RECOLECCIÓN DE EVIDENCIAS DOCUMENTALES ELECTRÓNICAS EN LA INDAGACIÓN PREVIA E INSTRUCCIÓN FISCAL

## 2.1 LA RECOLECCIÓN DE EVIDENCIAS DOCUMENTALES ELECTRÓNICAS EN LA INDAGACIÓN PREVIA

Es fundamental el estudio de las técnicas de la recolección de evidencias documentales electrónicas por parte del fiscal en la fase de Indagación Previa e incluso en la de Instrucción Fiscal, con el fin de que al momento de elevarla a prueba pueda tener eficacia y eficiencia; es decir, sirva de elemento que lleve a presumir de forma inequívoca la existencia del delito o la responsabilidad en los distintos grados de quien es acusado. Sin embargo, en el caso de la defensa si quiere utilizar uno de estos elementos deberá así mismo vigilar que el fiscal y los peritos cumplan con los requisitos y principios analizados en el capítulo anterior para asegurar que su valoración sea la esperada por parte de los miembros del Tribunal de Garantías Penales, ante quienes se evacuan la prueba.

Como ya lo analizamos, uno de los elementos que camina en contra de una teoría tradicional de las evidencias documentales, es la volatibilidad de los documentos electrónicos; es decir, se puede eliminar, modificar, alterar los mismos en segundos, y perderían para siempre el principio de integridad y autenticidad que es necesario para su valoración como prueba.

La Informático Forense es la rama que se preocupa por determinar cuál es la mejor forma de recolectar y tratar las evidencias informáticas, ya sean en forma de registros o mensajes de datos de equipos o dispositivos informáticos o electrónicos, con el fin de que las mismas permitan aclarar el hecho investigado, o coadyuven a obtener elementos que permitan esclarecer las circunstancias del delito o la responsabilidad de los procesados y ser elevados a prueba.

Es por estas razones que el Ministerio Público en su afán de dar las directrices necesarias a los Fiscales, y miembros de la Policía Judicial, ha elaborado un MANUAL DE MANEJO DE EVIDENCIAS DIGITALES Y ENTORNOS INFORMÁTICOS[31]. Este documento inicia por establecer su importancia y objetivos, luego pasa ha enumerar los cuatro principios básicos que regulan el manejo de este tipo de evidencias y que ha saber son:

- Ninguna acción debe ser tomada para que cambie o altere la información almacenada en soportes informáticos y sea presentada ante el Tribunal.

- Por excepción una persona capacitada puede acceder a la información original, detallando lo realizado, su justificación y las implicaciones de dichos actos.

- Llevar una Bitácora de los procesos relacionados con los adelantos en la investigación de este tipo de evidencia, para que un tercero pueda recrear y obtener el mismo resultado obtenido en el primer análisis.

- El Fiscal y el oficial son responsables por cumplir con la ley para la posesión y el acceso a la información almacenada, así como en el caso que una persona acceda y copie la información.

Al momento de la recolección de evidencia digitales es necesario determinar el tipo de delito; es decir, si la investigación se trata de un delito que tenga a la informática o electrónica como medio para su comisión, o sea un delito fin, como delito electrónico, ya que difiere la forma de obtener y recolectar las evidencias y ser usadas.

Así mismo se hace necesario reconocer las diferencias entre las evidencias digitales, y las evidencias electrónicas, ya que las primeras se

[31] ACUARIO del Pino, Santiago; "MANUAL DE MANEJO DE EVIDENCIAS DIGITALES Y ENTORNOS INFORMÁTICOS" Fiscalía General del Estado, 2009

refieren al software o la información, y las segundas al hardware o componentes físicos, haciendo de esta manera una distinción también entre la escena digital y la escena física.

A continuación este manual explica como se debe diferenciar unos de otros:

| SISTEMA INFORMÁTICO | |
|---|---|
| **HARDWARE** (Elementos Físicos) | **Evidencia Electrónica** |
| • El hardware es mercancía ilegal o fruto del delito. | • El hardware es una mercancía ilegal cuando su posesión no está autorizada por la ley. Ejemplo: en el caso de los decodificadores de la señal de televisión por cable, su posesión es una violación a los derechos de propiedad intelectual y también un delito.<br>• El hardware es fruto del delito cuando este es obtenido mediante robo, hurto, fraude u otra clase de infracción. |
| • El hardware es un instrumento | • Es un instrumento cuando el hardware cumple un papel importante en el cometimiento del delito, podemos decir que es usada como un arma o herramienta, tal como una pistola o un cuchillo. Un ejemplo serían los snifers y otros aparatos especialmente diseñados para capturar el tráfico en la red o interceptar comunicaciones. |
| • El hardware es evidencia | • En este caso el hardware no debe ni ser una mercancía ilegal, fruto del delito o un instrumento. Es un elemento físico que se constituye como prueba de la comisión de un delito. Por ejemplo el scanner que se uso para digitalizar una imagen de pornografía infantil, cuyas características únicas son usadas como elementos de convicción |

| SISTEMA INFORMÁTICO | |
|---|---|
| **INFORMACIÓN** | **Evidencia Digital** |
| • La información es mercancía ilegal o el fruto del delito. | La información es considerada como mercancía ilegal cuando su posesión no está permitida por la ley, por ejemplo en el caso de la pornografía infantil. De otro lado será fruto del delito cuando sea el resultado de la comisión de una infracción, como por ejemplo las copias pirateadas de programas de ordenador, secretos industriales robados. |
| • La información es un instrumento | La información es un instrumento o herramienta cuando es usada como medio para cometer una infracción penal. Son por ejemplo los programas de ordenador que se utilizan para romper las seguridades de un sistema informático, sirven para romper contraseñas o para brindar acceso no autorizado. En definitiva juegan un importante papel en el cometimiento del delito. |
| • La información es evidencia | Esta es la categoría más grande y nutrida de las anteriores, muchas de nuestras acciones diarias dejan un rastro digital. Uno puede conseguir mucha información como evidencia, por ejemplo la información de los ISP's, de los bancos, y de las proveedoras de servicios las cuales pueden revelar actividades particulares de los sospechosos |

El manual también establece una metodología dirigida a quien realice una investigación forense, y recomienda primero buscar en las fuentes de evidencias digitales, las mismas que se clasifican en tres grupos:

**Sistemas de computación abiertos**: Se refiere principalmente a lo que se denomina computadoras personales y sus componentes, los mismos que guardan gran cantidad de información.

**Sistemas de comunicación:** Se refiere a las redes o instalaciones ya sean inalámbricas, telecomunicaciones o Internet.

**Sistemas convergentes de comunicación:** Son sistemas que unen los dos anteriores y que poseen la capacidad de almacenar gran cantidad de información. Se refiere a los Aifons, Pds, etc.

Estas evidencias también nos pueden permitir conocer a la persona que es investigada, debido a que se pueden elaborar perfiles sobre gustos, conocimientos, intereses, etc.

Se recomienda en el manual que al momento de llegar a la escena del crimen se realice lo siguiente:

1. Determinar si el delito esté en progreso, si no lo está, se debe proceder a reconocer el lugar donde se produce, tomando dimensiones y haciendo un detalle de las cosas que se encuentren en este lugar. Si existen evidencias electrónicas, es necesario proteger los aparatos y sistemas de información.

2. Hay que determinar la seguridad dentro de la escena, tanto de seguridad personal como de riesgos eléctricos, químicos, o biológicos.

3. Asegurar físicamente; retirando a las personas extrañas, evitando accesos no autorizados, o contaminación de las evidencias.

4. Asegurar físicamente a las evidencias, con el fin de mantener la cadena de custodia, guardando y etiquetando cada elemento.

5. Cumplido lo anterior se puede entregar la escena del crimen a la autoridad.

6. Documentar la explotación de la escena, tomando nota de los detalles de la misma en una bitácora de los hechos, evidencias obtenidas y su posible relación con el sospechoso.

Cuando en la escena ya se determinen los elementos electrónicos de evidencia es necesario tomar en consideración los pasos en el reconocimientos de los mismos, por lo que es necesario, no desconectar los elementos de inmediato y si están apagados no prender, evitar que se bloqueen los

computadores, manipular con guantes, ponerlos en condiciones de seguridad, y llamar a un técnico de inmediato.

El manual determina los actuares según el tipo de tecnología, los cuales son útiles ya que buscan conservar la evidencia de forma íntegra, auténtica, original, y precautelar la misma en el transcurso de la investigación, procedimientos que resultan sumamente importantes para este tipo de delitos que utilizan o son el blanco de ellos los medios tecnológicos.

## 2.2 LA AUTORIZACIÓN DE LOS JUECES DE GARANTÍAS PENALES PARA RECOLECCIÓN DE EVIDENCIA.

En la etapa de investigación se vuelve necesario cuidar la forma de acopiar las evidencias tecnológicas y de información con el fin de que estas adquieran valor como prueba, sin embargo para esto, es necesario cuidar que las mismas sean legales.

El Código de Procedimiento Penal, determina la necesidad de acudir ante el Juez de Garantías Penales, con el fin de obtener autorizaciones para acceder, revisar, guardar, retirar bienes o información, cuando esta sea necesaria para la investigación del delito.

La razón para solicitar autorizaciones no solamente se limita a las establecidas en el código adjetivo penal, sino que tienen un antecedente en el ejercicio de los derechos constitucionales y a los principios que los rigen, ya sea el secreto de correspondencia, que protege la libertad de expresión, la igualdad formal, el honor, la imagen, etc. Derechos con rango así mismo constitucional que protegen a la persona y permiten su desarrollo como sujetos sociales.

Son importantes estas autorizaciones, con el fin de que tenga valor jurídico las pruebas obtenidas, ya que caso contrario lo carecería de acuerdo a lo dispuesto en el Art. 83 del Código Penal y el numeral 4 del Art. 76 de la Constitución.

### 2.2.1 LA INCAUTACIÓN DE EVIDENCIAS MATERIALES

El Art. 93 del Código de Procedimiento Penal regula esta diligencia. La Incautación se entiende "*como privar a alguien de alguno de sus bienes como consecuencia de la relación de estos con un delito, falta o infracción administrativa*"[32].

Esta diligencia es importante para recopilar prueba material, principalmente para poder custodiar y tener los objetos de comisión del delito como serían las armas, herramientas, computadoras, cajeros, servidores, decodificadores, etc. y las que determinen la responsabilidad de las personas. Sin embargo puede resultar así mismo imperioso conjuntamente solicitar una oren de allanamiento del lugar en donde se encuentre las cosas, caso contrario puede producirse una violación de domicilio.

También puede tratarse de incautar papeles, esto en el sentido tradicional, por que se si trata de documentos electrónicos no cabe la incautación, porque estos están desmaterializados.

Luego de la incautación debe necesariamente producirse el reconocimiento y descripción de los objetos o documentos con la intervención de peritos, diligencia que se deja reducida a un acta elaborada por el secretario de la Fiscalía que da fe y la suscribe al igual que el fiscal y los peritos. Luego pasa a custodia de la Policía Judicial. Se puede devolver al propietario o terceros poseedores o a quien les corresponda con la condición de avaluar, reconocer y describir el bien. Se puede devolver al Acusador, ofendido o

[32] VACA Andrade, Ricardo, "Manual de Derecho Procesal Penal", Editorial Catedral y Corporación de Estudios y Publicaciones, Cuarta Edición, Tomo 1, Quito Ecuador, pág. 899

tercero a condición de que se vuelva a presentar cuando la Fiscal, Juez o Tribunal lo ordene.

### 2.2.2 LA APERTURA DE CORRESPONDENCIA ELECTRÓNICA

El numeral 21 del Art. 66 de la Constitución de la República, garantiza el derecho de inviolabilidad de la correspondencia virtual; es decir, de los e-mails o correos electrónicos de la misma forma que el correo epistolar.

Por esta garantía y desde mucho antes, la necesidad de apertura de una correspondencia requiere necesariamente la autorización de un Juez de Garantías Penales, como lo dispone el Art. 150 del Código de Procedimiento Penal.

*Art. 150.- Inviolabilidad.- La correspondencia epistolar, telegráfica, telefónica, cablegráfica, por télex o por cualquier otro medio de comunicación, es inviolable. Sin embargo el juez podrá autorizar al Fiscal, a pedido de este, para que por sí mismo o por medio de la Policía Judicial la pueda retener, abrir, interceptar y examinar, cuando haya suficiente evidencia para presumir que tal correspondencia tiene alguna relación con el delito que se investiga o con la participación del sospechoso o del imputado.*

Esta norma consagra una excepción al derecho de inviolabilidad de correspondencia, cuyo núcleo principal resulta difuso; es decir, para algunos es considerado la libertad, principalmente la de expresión y para otros protege el derecho de intimidad y de privacidad. Se habla también que este derecho es intermedio, es decir protege de eventuales ataques a otros derechos constitucionales difusos. Sin embargo, en ese caso la necesidad de la investigación delictual puede permitir un conocimiento del contenido de la información, para verificar la existencia de una infracción y sancionar a los responsables.

Pero **¿Que es un correo electrónico? "***Técnicamente, un correo electrónico es información contenida en un dispositivo de almacenamiento magnético que puede ser transmitido de un ordenador a otro a través de sistemas de redes de ordenadores. Un correo electrónico está formado por dos partes o tipos de información. Una primera denominada información de control, compuesta por la fecha de envío, destinatario, ordenador desde donde parte el correo y otras informaciones de carácter técnico, como por ejemplo la ruta de ordenadores que ha seguido el correo para llegar hasta su destino. Y una segunda información de carácter más personal, que es el asunto y el contenido o texto del mensaje. Esta información contenida en dispositivos de almacenamiento magnéticos es gestionada por programas informáticos de correos que traducen esa información almacenada en palabras, imágenes y sonido. Lo importante de un correo electrónico es precisamente su contenido, las palabras, las imágenes la información. Podría decirse que un correo electrónico es una carta, un paquete, que viaja abierto si éste no ha sido encriptado. Es un medio de transmitir información, de una persona a otra o de una persona a un grupo de personas a través de redes."*[33]

La autorización se otorga para algunos supuestos entre estos: retención, apertura, intercepción y examen, debe ser realizada por el fiscal, sin embargo a veces se encomienda la actuación a los miembros de la policía nacional, lo cual podría afectar al principio dispositivo y por lo tanto los resultados de la investigación.

A continuación es necesario analizar algunos de estos supuestos:

**INTERCEPTAR:** La Real Academia de la Lengua Española, define como: **"1.** tr. Apoderarse de algo antes de que llegue a su destino. **2.** tr.

[33] BLÁZQUEZ, Blanca E. "Aspectos Jurídicos Sobre el Control del Uso del Correo Electrónico por parte de las Empresas en el Ámbito Laboral", mgabogados.com, información jurídica, http://www.mgabogados.com/despacho/controldelemail.htm

Detener algo en su camino. **3.** tr. Interrumpir, obstruir una vía de comunicación"[34] la intercepción de la correspondencia, se refierea a la posibilidad de desviar antes de que llegue al destinatario, u obstaculizar la via de comunicación y/o apoderarse de la misma, entendido el apoderamentiento no solamente como la toma material del sobre, sino incluso cuando se quita del poder del dueño ya sea escondiendo o reteniendo por un tiempo prolongado. Como podermos observar en el mundo virtual es dificil hablar de un apoderamiento material, lo que se puede es desviar la información y evitar que llegue a sus destinatario, esto precisamente porque lo que viaja es información desmaterializada, trasmitida en un lenguage especial llamado *protocolo SMTP*[35] y con un encabezado que lleva datos de remitente, destinatario y la ruta seguida, sin embargo algunos proveedores de correspondencia, y programas representan visualmente la llegada de un mensaje de correo nuevo en un sobre el cual se encuentra cerrado y al mirar el contenido se observa ya el sobre abierto, pero el correo virtual no es el sobre, sino es una forma de comunicación de un mensaje de datos en tiempo no real, entre dos o mas personas, en un lenguage especial y que puede o no estar representada gráficamente en sobres.

La Retención necesariamente acompaña a la intercepción, incluso se puede considerar un sinónimo de la primera; es decir, es detener en algun lado la correspondencia, con el fin de tomar posesión de ella y evitar que llegue a su destinatario, claro esto en el sentido material; sin embargo, en el campo virtual puede ser factible, ya que los protocolos de comunicación o lenguage en especial el IP, forma paquetes de comunicación que pueden ser retenidos, pero existen medidas técnicas que duplican estos paquetes para que vayan por distintos caminos y en un servidor se completen y puedan legar al destinario, es decir si se pierde un paquete se puede recuperar por esta duplicación, por lo tanto lo que se podría realizar es un copia, por la intercepción.

[34] DICCIONARIO DE LA LENGUA ESPAÑOLA" Vigésima segunda edición on line http://buscon.rae.es/draeI/

[35] KIOSKEA NET"Cómo Funciona el Correo Electrónico" http://es.kioskea.net/contents/courrier-electronique/fonctionnement-mta-mua.php3

A la apertura, la debemos entender en el verbo **Abrir:** La Real Academia de la Lengua Española, establece algunas definiciones entre ellas: **1.** tr. Descubrir o hacer patente lo que está cerrado u oculto. **6.** tr. Dejar en descubierto algo, haciendo que aquello que lo oculta se aparte o se separe. *Abrir los ojos,* por separar un párpado de otro. *Abrir un libro,* por separar una o varias de sus hojas de las demás para dejar patentes dos de sus páginas. **9.** tr. Extender lo que estaba encogido, doblado o plegado. **10.** tr. Hender, rasgar, dividir. **12.** tr. Despegar o romper por alguna parte una carta, un paquete, un sobre, una cubierta, etc., para ver o sacar lo que contengan.[36]

Implica esta acción que el objeto necesariamente esté cerrada *no con el riguroso sentido técnico postal, sino que la correspondencia, esté asegurado de modo que no pueda imponerse de ella sin vencer alguna resistencia material. Por lo tanto cerrado no implica que el sobre esté engomado o sellado, sino también la que es cuidadosamente doblada para incluirla en un pliego acompañado de manuscrito, o en un impreso, bajo cubierta amarrada con cordel, con uno o varios nudos.*[37] Por tanto no podrá ser objeto de esta acción las postales que viajan abiertas y sin sobre. La correspondencia virtual, como lo manifestaba viaja abierta, por lo tanto no podría ser objeto de apertura, sin embargo puede ser abierta, ya que se requiere hacer clic o aceptar su apertura, sin que necesariamente se solicite claves o otros medios de seguridad, estos son aplicados para ingresar al programa o sistema que gestiona el e mail, o cuando el mensaje viaja cifrado.

Por último, la norma habla de examen; es decir, se entiende no solo como su lectura, sino que va más allá, es aplicar un ejercicio mental para comprender no solo las palabras sino su contexto, por lo tanto implica un estudio, Caballas considera que es el momento en donde el Fiscal toma contacto directo y conocimiento detenido y analítico del contenido del

[36] DICCIONARIO DE LA LENGUA ESPAÑOLA" Vigésima segunda edición on line http://buscon.rae.es/draeI/
[37] MARGGIORE, GIUSEPPE "Derecho Penal IV Delitos en Particular" Segunda Edición, Editorial Temis Bogotá, 1972

documento para descubrirlo, con el fin de obtener información eficaz para la investigación y que fue sopesada por el Juez de Garantías Penales como válida al momento de conceder la autorización.

El procedimiento necesario para la obtención de esta prueba es el siguiente:

- La **notificación al interesado,** para que conozca de la diligencia y concurra a la misma en compañía de su defensor, o decida no ir y se proceda a la apertura, examen y lectura de la correspondencia o el documento en forma reservada, notificación que debe ser realizada por el fiscal en una resolución que señala el día y hora en que deba cumplirse con la diligencia, dictada y notificada con la debida anticipación. Es necesario que se deje constancia de la realización del acto, con el fin de que no se alegue una violación de derechos en la adquisición de esta prueba. La notificación se vuelve necesaria para que la persona que pueda resultar afectada por esta actuación procesal esté enterada y pueda precautelar sus intereses o información que pueda ser divulgada a través de la publicación de esta correspondencia en un proceso penal.
- Apertura de la correspondencia. Al tratarse de correspondencia virtual se hará necesario contar con la presencia de un perito informático para que tome las medidas necesarias con el fin de que la información de llegada, almacenamiento, fechas y horas no se altere.
- Examen de la Correspondencia; la misma que se realiza de forma privada y con la ayuda de un perito para cuidar la integridad de la prueba.
- Incorporación al proceso; del examen que realiza el fiscal sí se concluye que los documentos o en la información está relacionada con la investigación, está documentación rubricada por el fiscal y el secretario debe agregarse al expediente. Si la correspondencia es virtual, la firma y rúbricas del secretario deberá realizarse por firmas electrónicas, y además al ser necesaria su impresión se podría así mismo rubricar e incorporarla en el expediente. En el caso de la prueba en forma

electrónica la firma del fiscal y secretario deberá realizarse de forma que no dañe el contenido de la información técnica de datos de llegada o almacenamiento.

- Devolución al interesado: si la información a criterio del fiscal no está relacionada con la investigación deberá devolverla al interesado. En el presente caso, lo que se hará es devolver el mail a su cause y llegue al interesado.

Por lo tanto, para que proceda a este tipo de diligencia es necesario las siguientes condiciones:

1. Que exista suficiente evidencia para presumir que tal correspondencia tiene alguna relación con el delito que se investiga o con la participación del procesado.
2. El Juez de Garantías Penales autorice al Fiscal la ocupación, apertura y examen de la correspondencia o documento.
3. Que el Fiscal haya notificado al interesado señalando día y hora para la práctica de la diligencia que debe ser reservada.
4. Que quienes conozcan sobre los contenidos de la diligencia, guarden secreto sobre lo conocido y que esta información obtenida no pueda ser utilizado por un tercero.

### 2.2.3 LA INTERCEPCIÓN DE MENSAJES DE DATOS.

El Art. 152 del Código Penal regula esta diligencia, que está acorde a la garantía constitucional establecida en el numeral 21 del Art. 66 de la carta fundamental, protege a cualquier forma de comunicación, en este caso se aplicarían para los mensajes de datos que sean trasmitidos por medios electrónicos, en esta categoría estarían los SMS o mensajes de celular, los faxs, los mensajes de bipers, telegrama, aunque estas tecnologías casi han desparecido.

El Art. 152 del Código de Procedimiento Penal, también se aplicaría a los documentos electrónicos que no sean transmitidos, es decir a los mensajes de datos, creados, generados, almacenados en medios electrónicos.

Esta protección se puede considerar un principio intermedio; es decir, con el fin de no violentar derechos fundamentales tales como la libertad de expresión, la intimidad, privacidad, etc.

La intercepción de mensajes de datos se debe entender en el mismo sentido que la correspondencia, por lo tanto, no solo será necesarios medios técnicos sino de peritos que puedan lograrlo y dotar de integridad con el fin de que luego pueda ser valorado por el Tribunal en la etapa de juicio.

El procedimiento sin embargo cambia respecto a la correspondencia en solamente un detalle, ya que igual que las misivas, es necesario contar con la presencia del procesado o su defensor, y si ellos notificados no concurren se puede contar con dos testigos que guarden reserva sobre lo visto. Se realizar un acta en la que firman los concurrentes, y si se encuentra información relevante a la investigación se la agrega al expediente una vez rubricada por el fiscal.

### 2.2.4 EL RECONOCIMIENTO DE DOCUMENTOS ELECTRÓNICOS.

El Art. 156 del Código de Procedimiento Penal, permite esta diligencia que permite al Fiscal proceder a reconocer los documentos electrónicos constantes en registros informáticos, siempre que estos hayan sido autorizados por el Juez de Garantías Penales para su retención en el caso de información desmaterializada o incautación si se trata de cosas materiales que contengan documentos electrónicos.

El reconocimiento entendido en términos generales, propende a que su dueño o quien conoce si es de su propiedad o de su conocimiento; sin embargo, en este caso la diligencia tiene como fin conocer los contenidos y no

reconocer, por lo tanto el nombre no es acorde con el fin mismo de la diligencia. Sin embargo al ser necesario la presencia de las partes con juramento para que guarden reserva sobre lo dicho, permite que el procesado pueda reconocer la evidencia que se presenta, siempre que así lo desee. En esta diligencia se vuelve necesaria la presencia de dos peritos, lo cual es lógica ya que las evidencias enumeradas para que sean reconocidas requieren de tecnologías precisas para su reproducción y lectura.

Por lo tanto la presencia de los peritos es para poder efectuar la diligencia, y si se trata de grabaciones como lo dispone el Art. 155 del Código de Procedimiento Penal, autorizada la grabación por el Juez de Garantías Penales previo a ser obtenida y luego de realizada, se procedería en esta diligencia a conocer su contenido y a su trascripción. En el aspecto informático es posible una grabación digital tanto de llamada telefónicas en tecnología voz sobre IP como las que se producen en programas como Skype o chats populares de Yahoo, Hotmail, o simplemente grabaciones en cd, o grabadoras digitales.

## 2.3 EL ANÁLISIS PERICIAL DE LAS EVIDENCIAS ELECTRÓNICAS.

Como hemos analizado en el primer capítulo de este trabajo de investigación, la pruebe electrónica por disposición de la Ley de Comercio Electrónica y por la lógica general de las cosas requiere necesariamente ser analizada por expertos, lo cual garantiza no solo la integridad de la prueba, sino de la misma investigación, ya que si se trata de evidencia concluyente que determine la existencia de la infracción y/o la responsabilidad del proceso, será de gran utilidad.

Como sabemos los avances tecnológicos y la complejidad de los conocimientos utilizados para su creación y funcionamiento, hacen que el análisis de la misma esté reservado a personas con conocimientos científicos y técnicos de alto grado, por lo que en el ámbito investigativo policial ya existen centros especializados, lo que demanda gran cantidad de recursos económicos, tecnológicos y humanos.

En el país la Policía Judicial a hecho esfuerzos en formar policías y funcionarios del Ministerio Público al respecto, a pesar de que las capacidades están limitadas ante la falta de tecnologías de puntas y de recursos humanos para realizar las investigaciones con mejores resultados. Sin embargo la misma complejidad de las comunicaciones y de la estructura del Internet, entendida como una telaraña mundial, hacen que alguna información depositada en servidores de dominio privada de otros países, sea difícil en su acceso, por lo que no solo se requiere capacidad mental, sino también física y legal, que será posible con la firma de convenidos internacionales de persecución del delito informático, como en los casos de convenios de persecución al narcotráfico y lavado de dinero, ya que podemos observar que los delitos en general y los delitos electrónicos van en aumento y utilizan los medios de comunicación y en especial el Internet como herramienta dentro de su comisión o para su ocultamiento.

Ya en el tema, el Art. 148 del Código de Procedimiento Penal dispone que cuando la prueba documental sea impugnada se podrá ordenar la prueba pericial, con la intervención de la policía judicial. Por lo tanto si los documentos electrónicos son impugnados en su validez, veracidad o integridad, será necesario contar con un perito que informe al Fiscal, si la evidencia obtenida puede ser considerada relevante para determinar la existencia de la infracción o establecer la responsabilidad.

Al analizar la norma, parece que este tipo de análisis solamente puede ser realizado por la policía Judicial, lo cual limita de sobremanera los resultados que se puedan obtener, ya que al ser una institución con limitados recursos, hace que los resultados no sean de todo satisfactorios. Es necesario anotar que existen profesionales a nivel nacional que se han formado de mejor forma, las universidades han demostrado contar con personal de alto nivel en el tema tecnológico, por ello el país ha logrado forma empresarios en programación de software con una visión mundial y estos productos del talento humano son de exportación.

Para Ribas[38] las limitaciones en la actividad investigativa de la prueba electrónica son las siguientes:

- Escasez de los medios técnicos dedicados a la actividad investigativas.
- Ventaja tecnológica de los delincuentes profesionales.
- Exceso de tiempo trascurrido entre la solicitud de un mandamiento de intercepción electrónica y su concesión y trámite.
- Uso de contramedidas, como el cifrado de la información y los sistemas de anonimato real.
- Problemas de jurisdicción en los delitos transfronterizos.

[38] Citado por RIOFRÍO Juan Carlos, “La Prueba Electrónica” Editorial TEMIS S. A. Bogotá Colombia, 2004, pág. 145.

Los peritos según el Código de Procedimiento Penal están definidos así: *Art. 94.- Peritos.- Son peritos los profesionales especializados en diferentes materias que hayan sido acreditados como tales, previo proceso de las Direcciones Regionales del Consejo de la Judicatura.*

***Art. 95**.- Informes periciales.- Durante la indagación previa, o en la etapa de instrucción, los peritos realizarán informes sobre la experticia realizada. Este documento lo incorporará el fiscal en el expediente y el defensor lo exhibirá durante la etapa intermedia.*

*Si hubiere peligro de destrucción de huellas o vestigios de cualquier naturaleza en las personas o en las cosas, los profesionales en medicina, enfermeros o dependientes del establecimiento de salud a donde hubiere concurrido la persona agraviada, tomarán las evidencias inmediatamente y las guardarán hasta que el fiscal o la Policía Judicial dispongan que pasen al cuidado de peritos para su examen.*

*Si se tratare de exámenes corporales, la mujer a la cual deban practicárselos podrá exigir que quienes actúan como peritos sean personas de su mismo sexo.*

*El Consejo de la Judicatura fijará las escalas de remuneración de los peritos.*

El peritaje pide quien necesita una opinión experta, objetiva e independiente sobre un tema en especial, científico, técnico o artístico. En el caso de los documentos electrónicos en el área de la informática, electrónica y las comunicaciones, son los conocimientos específicos en el área técnica y porque no científica, cuando se vuelve necesario desencriptar y analizar la información. En el caso de nuestra normativa jurídica la designación la realiza el fiscal.

Su designación es trascendental ya que no solamente es necesario encargar este acometido a quien posee los conocimientos especializado sobre

algún campo de la informática, sino los instrumentos, equipos y la experiencia profesional necesaria, así como quien tenga conocimientos sobre el proceso penal y formas de realizar el informe.

Una vez designado, notificado y posesionado el perito se hace necesario que el mismo siga una metodología para el análisis de los datos que será:

- Identificación de los elementos que deben ser analizados.- Lo que se refiere a identificar el hadware, redes o sistemas; luego se deberá proceder a analizar el contenido de infracción en análisis de datos, sobre las palabras que deben ser especificadas por el Juez, el documento relacionado o imágenes; la identificación de los datos cronológicos de creación, acceso o modificación de archivos y documentos electrónicos. Entradas y salidas de usuarios y acceso a historial web. Así mismo es necesario que determine el equipo necesario para ejecutar la información, los tipos de almacenamiento, etc.

- Preservar los datos.- Es un aspecto importante a tomar en cuenta, debido a que le es indispensable tomar medidas con el fin de que no se borre la información, por lo que deberá determinar quien tiene el control de sistema, recolectar evidencia material, como discos, dispositivos, etc, sacar imágenes del disco duro o snapshot, copiar respaldos, custodiar los equipos, ya que no toda la información es posible de reproducir en cualquier equipo debido a incompatibilidades o puede estar protegida por claves o encontrarse encriptadas. Existen manuales que recomiendan incautar los discos duros y dejar al usuario solamente una copia. También será necesario copiar el software y los bios (información que es contenida en un chip y que identifica a la máquina y su funcionamiento). Sin embargo, por la volatibilidad de la información su simple acceso puede alterarla, borrarla o destruirla. Es necesario que los peritos cuenten con firmas electrónicas o apliquen funciones hash para mantener la información intacta y demostrar esto cuando sea el momento de comparecer ante el Tribunal.

- Analizar los datas.- Ya sea encontrando conexiones entre la información almacenada y la de la investigación fiscal, se puede reconstruir lo borrado, encontrar información precisa, etc.

- Emitir el dictamen; lo cual es importante ya que en el mismo además de los requisitos de ley, se debe explicar los procedimientos para obtener la información, el software usado y su confiabilidad, las conclusiones. Deberá ser redactado en lenguaje sencillo, o explicarse los tecnicismos, con gráficos. También es necesario establecer las limitaciones producidas.

***Art. 98**.- Contenido del informe pericial.- El informe pericial contendrá:*

*1. La descripción detallada de lo que se ha reconocido o examinado, tal cual lo observó el perito en el momento de practicar el reconocimiento o examen:*

*2. El estado de la persona o de la cosa objeto de la pericia, antes de la comisión del delito, en cuanto fuere posible;*

*3. La determinación del tiempo probable transcurrido entre el momento en que se cometió la infracción y el de la práctica del reconocimiento;*

*4. El pronóstico sobre la evolución del daño, según la naturaleza de la pericia;*

*5. Las conclusiones finales, el procedimiento utilizado para llegar a ellas y los motivos en que se fundamentan;*

*6. La fecha del informe; y,*

*7. La firma y rúbrica del perito.*

*En el caso de que hubiesen desaparecido los vestigios de la infracción, los peritos opinarán, en forma debidamente motivada sobre si tal desaparición ha ocurrido por causas naturales o artificiales. Esta opinión deberá sujetarse a los principios del debido proceso y la presunción de inocencia.*

*El procesado tiene derecho a conocer oportunamente el informe pericial, a formular observaciones y a solicitar aclaraciones al perito, sin perjuicio de su derecho a interrogarle en la audiencia.*

# CAPITULO III

# LA PRUEBA DOCUMENTAL ELECTRÓNICA EN LA ETAPA DE JUICIO

## 3.1 LA PRESENTACIÓN DE LA PRUEBA DOCUMENTAL ELECTRÓNICA.

Una vez que se haya concluido la etapa intermedia con el auto de llamamiento a juicio, se inicia la etapa de juicio en donde se va a absolver o a condenar al procesado; se la considera la etapa cúlmen del proceso penal, esto debido a que las otras dos etapas anteriores y la de investigación preprocesal tienen por finalidad recopilar la información suficiente para imputar de la comisión de un delito en el grado de autor, cómplice o encubridor al procesado o en la que se ratifique su inocencia.

Es en esta etapa en donde todos los indicios, deben convertirse en pruebas para establecer hechos que determinen la comisión de un delito o impliquen la responsabilidad del procesado. Todos los esfuerzos investigativos de las anteriores etapas se exponen y buscan ser claros, precisos y concordantes con el fin de sustentar un fallo por parte del Tribunal de Garantías Penales.

Sin embargo la prueba que va a ser practicada y despachada en esta etapa debe ser anunciada en la Audiencia Preparatoria de Juicio de la Etapa Intermedia, en donde los sujetos pueden formular solicitudes, observaciones, objeciones y planteamientos que estimaren relevantes referidos a la oferta de prueba realizada por los demás intervinientes. Así como también es en este momento donde corresponde al Juez de Garantías Penales, resolver sobre las solicitudes para la exclusión de las pruebas anunciadas, cuyo fundamento o evidencia que fueren a servir de sustento en el juicio, hubieren sido obtenidas violando las normas y garantías determinadas en los instrumentos internacionales de protección de Derechos Humanos, la Constitución y en el Código de Procedimiento Penal. En este momento los indicios electrónicos que hayan sido recolectados con vicios de legalidad; es decir, sin las autorizaciones

-ya analizados en el capítulo anterior- o de constitucionalidad, ya sea por violentar derechos de secreto de comunicaciones y correspondencia, datos personales, o por violaciones al debido proceso no pasan a la siguiente etapa.

Este también será el momento de solicitar registros informáticos que requieran autorización judicial para su petición, como por ejemplo registros bancarios, de datos personales, etc. y que no puedieron ser conseguidos, esto principalmente para los defensores o acusadores particulares, cuando los fiscales no lo hayan hecho en la etapa anterior.

Sin embargo, de la reforma de marzo de 2009, aún se mantiene vigente la disposición del Art. 267 del Código de Procedimiento Penal, que permite anunciar lista de testigos y pedir las demás pruebas a fín de que se practiquen durante la audiencia, con tres días de anticipación a la reunión del Tribunal, siempre que no hubieren sido anunciadas y discutidas en la audiencia preparatoria del juicio. Las objeciones sobre las mismas se hacen en la Audiencia de Juicio.

Por lo tanto, se deberá necesariamente anunciar en cualquiera de los dos momentos indicados en líneas anteriores, el listado de testigos expertos informáticos y las pruebas materiales en donde se incluirán los elementos materiales de la información, tales como CPU, celulares, Aifons, y cualquier elemento físico de la red, los sopertes electrónicos en donde conste la prueba a ser reproducida, CD, USB o memorias flash, discos duros, discos externos, etc., los mismos que ya debieron ser recolectados en la etapa de investigación y/o en la de instrucción fiscal.

Por lógica general, la prueba documental por si sola ya no tiene una relevancia importante en el sistema acusatorio oral, lo que sucede es que al ser oral, se requiere que la misma se acotada y corroborada por los testimonios o peritos, quienes son los indicados para introducir estos elementos materiales, pese a que ya puedan constar en el expediente.

Considero importe manifestar que los documentos electrónicos que van a ser presentados como prueba deben encontrarse impresos en lo posible, en el caso de video requeria mucho papel y tiempo, por lo que será importante conste detallado en el informe del perito con las capturas de imágenes más importantes, y además se agregen en formato electrónico, con el fin de garantizar su reproducción; en el audio destaca la transcripción realizada por el perito en la diligencia de reconocimiento. Es necesario que la parte que presenta esta clase de prueba facilite los elementos necesarios para su reproducción, por lo que se vuelve sumamente importante con el fin de que el Tribunal presencie por si mismos los indicios ya examinados por un perito, garantizando de este modo la inmediación, y por tanto el mejor exámen que haga el Tribunal a esta prueba.

Una vez iniciada la Audiencia de Juicio, el Fiscal debe iniciar con el alegato de entrada y luego solicitar la prueba, en donde debe necesariamente presentar las pruebas materiales y las documentales, y en el caso de la prueba documental electrónica se hará necesario presentar los soportes electrónicos y los impresos.

Con los testigos solicitados, se puede reconocer los elementos materiales e incluso los documentos electrónicos; por ejemplo, un registro informático, una página web, un mail, etc., solicitando al Tribunal permiso para exhibirlo y luego agregarlo al proceso, en el formato electrónico y en un impreso, ya sea del documento o en captura de imagen; la forma de mostrar será sirviéndose de un elemento de reproducción, ya sea una pantalla con un infocus u otro aparato electrónico, por no ser posible el cambio de formato o evitar su alteración.

Las preguntas que haga el Fiscal, si es testigo de cargo, o el defensor si es su testigo, deberán ser tendientes a reconocer no solo el aparato electrónico sino los contenidos de la información, si está alterada, qué fechas recibió o generó el documento electrónico, cuándo se dieron las modificaciones, si tiene seguridades el software para evitar cambios, formas de reconocer los usuarios de las computadoras, etc. Todas con el fin de demostrar su autenticidad e

integridad, así como la reproducción al poder ser mostradas a los miembros del Tribunal.

## 3.2 EL TESTIMONIO DEL PERITO PARA ACREDITAR UNA PRUEBA DOCUMENTAL ELECTRÓNICA.

El perito informático es un experto que tiene las posibilidades de examinar un documento informático y determinar si el mismo es auténtico, íntegro y reproducible. Lo que pretende la prueba es que se dote de una opinión experta, con credibilidad pero en términos generales y comunes que haga comprender estos conocimientos a los miembros del Tribunal, ya sea para comprobar o para juzgar hechos.

El perito se distingue de los testigos porque expone conocimientos especiales sobre la materia electrónica que el Tribunal o Juzgado no puede tener. Su vinculación es debido a sus conocimientos sobre el tema y no sobre los hechos que puedo conocer como lo es el testigo, así mismo el perito en su declaración emite un dictamen sobre sus conocimientos o experiencia y formula conclusiones, en el caso de los testigos en cambio su intervención es narrativa de lo que vieron, oyeron y presenciaron, no se admite conclusiones[39].

Si bien en las etapas anteriores pudo tener importancia, en la etapa de juicio es donde la parte que se puede beneficiar de sus manifestaciones va ha tener que hacer un esfuerzo para que la intervención del testigo experto y sus opiniones queden grabadas en la memoria del Tribunal por los aspectos relevantes que manifiesta y que puedan a partir de sus conocimientos especializados sustentar la teoría del caso presentada.

Una vez que se encuentre el testigo experto, es necesario garantizar su credibilidad, por lo tanto se deberá hacer preguntas tendientes a acreditarlo; es

[39] COUTURE, Eduardo, "Valoración Judicial de las Pruebas", Editorial Jurídica de Colombia, Tercera Edición, Colombia, 2008.

decir, que demuestre sus conocimientos y experiencia en lo que realiza, así será necesario preguntar sobre sus estudios, o conocimiento, años de trabajo, publicaciones, investigaciones, los procedimientos o métodos de investigación aplicados para llegar a las conclusiones que expresa.

Posterior se debe pasar a reproducir el testimonio, el orden de organización de las declaraciones ya no será cronológico sino temático, que cubra las distintas conclusiones y procedimientos llevados adelante para arribar a la misma conclusión[40]; en este caso será necesario tocar temas como, el hardware necesario, el software utilizado, seguridades, integridad y propiedades del documento electrónico, si puede ser determinada la autoría, fechas, horas, datos sobre la creación, modificaciones, lugares de envío y recepción, etc. Si las palabras utilizadas por el perito no son comunes sino técnicas es necesario se pregunte sobre su significado; en este momento es importante que el perito pueda presentar al Tribunal incluso con una práctica o demostraciones gráficas el procedimiento empleado y los resultados, esto debido a la complejidad del tema, lo que hace que las pequeñas demostraciones lleguen de mejor forma a los juzgadores y con ello se demuestra la reproducción de la prueba, principio necesario para ser valorado como elementos de convicción.

Así mismo, es fundamental que la persona que realiza el interrogatorio (Fiscal, abogado acusador o defensor) ponga especial relevancia sobre la forma de adquirir la prueba, si se siguió las recomendaciones del manual, analizado en el capítulo segundo, y de cómo estas recomendaciones al ser aplicadas garantizaron la integridad, autenticidad y la reproducción de la prueba en el momento del interrogatorio. También puede preguntarse sobre la legalidad en la recolección, pese a que el filtro sobre este tema ya se lo realiza en la Audiencia Preparatoria del Juicio.

Es necesario que se ponga gran interés en las conclusiones a las que llega, lo que puede determinar aspectos importantes para establecer las

[40] BAYTELMAN, Andrés: LITIGACIÓN PENAL Y JUICIO ORAL", Fondo de Justicia y Sociedad, Fundación Esquel- USAID.

responsabilidades de los procesados o su inocencia, a partir de hipótesis sobre las cuales emiten sus opiniones, no con el fin de probar los hechos, ya que no se trata de testigos presenciales, sino de expertos que pueden ayudar a determinar si las presunciones de las teorías del caso son ciertas o no, de acuerdo a los resultados obtenidos de los elementos de convicción.

Respecto al informe que realizó el perito anteriormente ya sea en la etapa de investigación o de instrucción puede servir para orientar el interrogatorio o encontrar fallas, para recordar al perito aspectos en donde se desea profundice, o para que muestre las evidencias que dan soporte a sus conclusiones. Con el actual sistema no se puede reproducir el mismo, sino es necesario que solamente sea una base que demuestre sus conocimientos.

En el contrainterrogatorio, la contraparte puede poner interés en desacreditar al perito en cuanto conocimientos, imparcialidad, en que no puede afirmar con certeza lo que dice debido a que los conocimientos están en constante cambio, los equipos informáticos y tecnologías cambian, se han encontrado fallas en los softwares utilizados, etc. También los cuestionamientos sobre las limitaciones en el aspecto tecnológico de máquinas o software para examinar la prueba suelen resultar interesantes ya que pueden desacreditar las hipótesis sobre el perito, por ello es necesario que la contraparte se haga asesorar de un técnico para planificar las preguntas del contrainterrogatorio, incluso puede estar presente para ayudar en el mismo al momento. También se puede intentar nominarle como testigo experto, sin embargo en la práctica los miembros de Tribunal no aceptan esto.

## 3.3 LOS PRINCIPIOS QUE RIGEN A LA PRUEBA ELECTRÓNICA DOCUMENTAL.

Este tema tiene especial relevancia al momento de ser valorada la prueba por parte de los miembros del Tribunal de Garantías Penales, que a

través de la sana crítica tiene que examinar las pruebas y sopesar si las mismas son claras, unívocas, precisas y concordantes y pueden sustentar un fallo absolutorio o condenatorio.

Una vez concluida la fase de debate en la Audiencia de Juicio, los miembros del Tribunal, deben pasar a deliberar en forma reservada, momento en el cual se debe proceder a examinar si la prueba electrónica presentada tiene valor o no.

Por lo tanto será necesario razonar sobre las hipótesis y conclusiones del perito y contrastar con las manifestaciones realizadas por los peritos legos, principalmente sobre los contenidos y sobre su existencia de la información, si esta es real o no. Con la prueba material presentada y reconocida si lo hizo el procesado, o por los testigos, lo que provocará que pase el test de unanimidad de los indicios.

Los principales elementos a ser debatidos son las conclusiones a las que llega el perito, los métodos utilizados para la obtención de la prueba y para su examen, sobre los resultados arrogados por la misma. Lo que hará que se pase el elemento de la claridad de los indicios.

La prueba documental para ser valorada en el tipo de proceso penal que tenemos, es decir en el sistema oral, debe ser necesariamente acreditada de forma verbal ante el Tribunal, sin embargo puede resultar importante que se refuerce las ideas que se dejó en esta forma por parte de los testigos y la prueba actuada en general, con las impresiones obtenidas, los informes, y el análisis de la misma prueba documental. En el caso de la prueba electrónica en forma de documento electrónico servirá en este momento las impresiones sobre sus contenidos, o capturas de imágenes, con el fin de que se sustente y confirme la convicción del juez pluripersonal que lo analiza.

En general la prueba documental como examiné en el primer capítulo de modo tradicional tuvo criterios en su valoración sobre la existencia del documento público y privado, el documento público con la división entre

auténtico y no auténtico. También se ha discutido sobre la originalidad y la copia, entre el documento firmado y no suscrito, anónimo, etc. Sin embargo, el documento electrónico puede llevar a que se discuta sobre estos mismos temas pero en forma diferente; es decir, la primera discusión será válida, porque existen documentos electrónicos públicos como lo establece el Art. 51 de la Ley de Comercio Electrónico, que dispone: *"Instrumentos públicos electrónicos.- Se reconoce la validez jurídica de los mensajes de datos otorgados, conferidos, autorizados o expedidos por y ante autoridad competente y firmados electrónicamente.*

*Dichos instrumentos públicos electrónicos deberán observar los requisitos, formalidades y solemnidades exigidos por la ley y demás normas aplicables*.

Sobre la originalidad o copia del documento electrónico, es un tema sumamente discutido, es decir la actual técnica permite en raras ocasiones determinar si el documento es una copia o es su original, sin embargo para esto servirá el criterio del experto. [41]

[41] Cita textual de CARRARA López, Valentín, "Valor Probatorio del Documentos Electrónico" UNED Centro Regional de Extremadura, MERIDA1995 pág. 148 hasta 153.

P*or un lado el documento gran parte en el disco magnético, al que llamamos documento electrónico, el mismo documento en soporte volátil, como la pantalla del monitor y a este documento lo imprimimos tendremos unos documentos uno sobre soporte magnético, otro sobre soportes fósforo, y el tercero sobre papel. ¿cuál de las tres es el documento original?, ¿Y los demás son copias?. El tema reviste trascendental importancia porque a las copias no se puede obligar a reconocerse, y tampoco puede hacerse pericias caligráficas tradicionalmente. Sin embargo cuando nos referimos a los documentos en soporte magnético, en la pantalla o en papel, solamente nos referimos a los soportes lo que cabe hablar son de documentos de primer grado, de segundo grado, en esta parte el documento o en soporte magnético del disco o sea de primer grado, y el impreso en papel en segundo grado pero ambos revestían a los efectos del reconocimiento, el carácter de originales. Se trata de documento original cuando se trata de un documento inicial, primitivo. Se habla de copias cuando se trata de la reproducción de un escrito. Un acto puede ser utilizado, ya sea en forma original, ya sea en forma de copias, pero al aplicar esto a las nuevas tecnologías de la información nos encontramos con que las copias nos conducen al problema de la distinción, del original. Para ciertos tratadista la distinción entre original y copia no tiene sentido en el cuaderno normal de los sistemas informáticos, por la simple razón de que no existió un original. Sobre este punto podemos distinguir claramente dos tendencias doctrinales:*

1. *Para una parte de los autores, los documentos informáticos pueden ser considerados como copias. Postura en que no podemos admitir ya que para que existan copias es necesario que existan original.*
2. *La para otros autores, el documento informático puede ser considerado como un original. Al respecto el Profesor Frayssinet, en su informe sobre las NTI, la*

*prueba y el sector público, sostiene que esta hipótesis es válida para la práctica instaurada en el conjunto del sistema jurisprudencial francés.*

*Pero adicionalmente la copia tiene mala prensa, lo que no hace más que expresar esta desconfianza cuando en presencia de copias, permite el cotejo del original. La poca calidad de las copias y los riegos de matriculación durante la operación de trascripción, justifican esta actitud. La segunda técnica y de organización que puede rodear a las operaciones de archivamiento electrónico defienden un cambio de mentalidad. En materia de documento electrónico es difícil distinguir el original de la copia, por lo qué algunas legislaciones se haya lanzado la necesidad de reconocer a la copia, la misma fuerza convincente que el original. Se ha teniendo en cuenta que la documentación corresponde al secretaria judicial que siguiendo los principios de la recomendación del concejo de Europa, debe conocer que los documentos conservados sobre soporte informático deben reunir las condiciones siguientes:*

1. *Ser la grabación fiel y duradera del documento original, al principio de la grabación por reproducción o codificación. Grabación por reproducción quiere decir la conservación del documento original en su forma gráfica y en su contenido. Grabación por codificación quiere decir la conservación del Documento original únicamente su contenido. Se considera duradera cualquier reproducción indeleble del original que ocasiona una codificación irreversible del soporte. Esta, es de tipo físico cuando se efectúa a nivel del soporte físicos del documento informático, o lógica cuando tiene lugar a nivel de métodos informáticos, utilizados para representar el documento.*
2. *Será efectuada de forma sistemática y sin laguna.*
3. *Será efectuada según la instrucción de trabajo, la conservas tanto en tiempo como las reproducciones o grabaciones.*
4. *Ser conservada con cuidado, en su orden sistemático y estar protegido contra cualquier tipo de alteración.*

*En el momento de grabación del original deben ser respetadas las siguientes reglas:*

1. *Los trabajos deben ser vigilados por el poseedor o depositario del documento, por una persona designada como responsable de la operación.*
2. *La grabación debe permitir determinar el orden de reproducción o codificación.*
3. *Las diversas fases de la grabación deben realizarse estrictamente, según las instrucciones de trabajo, que deberán ser conservadas tanto tiempo como las reproducciones o grabaciones.*
4. *La grabación de ser objeto de un acta conservada como la grabación. Debe responder a las indicaciones siguientes:*
   - *Identidad del operador responsable.*
   - *Naturaleza y tema de los documentos.*
   - *Lugar y fecha de la operación.*
   - *Defectos eventuales constatados durante la grabación.*
   - *La declaración firmada por el operador responsable en la que conste que los documentos han sido grabados de manera completa, regular y sin alteración: esta declaración puede sólo objeto de una grabación a continuación de los documentos grabados.*
5. *La grabación debe estar disponibles siempre para consulta de las personas legalmente habilitadas para tener acceso a los datos.*

*Las reglas siguientes son aplicables a los sistemas de tratamiento de documentos informáticos:*

1. *Los sistemas deben incluir las seguridades necesarias para evitar una alteración de grabaciones.*
2. *La los sistemas deben permitir restituir en cualquier momento a las informaciones grabadas barajó una forma legible directamente.*

*Las reglas siguientes aplican a los programas de tratamiento de documentos informáticos :*

Sin embargo, si se analiza la norma del Art. innumerado agregado a continuación del Art. 156 del Código de Procedimiento Penal, soluciona este problema al establecer que para que sean válidos, se debe garantizar su integridad, autenticidad y reproducción y no afecten en modo alguno los derechos y garantías fundamentales reconocidos en la Constitución y la Ley.

Así mismo en el primer y segundo capítulo ya se analizó de forma sucinta estos requisitos, y se explicó sobre la necesidad de la legalidad y constitucionalidad de las actuaciones de los Fiscales para obtener y examinar la prueba electrónica, sin embargo a continuación estudiaré los tres principales pilares de este tipo de prueba. La integridad, autenticidad y reproducción, lo que debe necesariamente sustentar y ser elementos de convicción para el Tribunal.

## 3.4 LA INTEGRIDAD DEL DOCUMENTO ELECTRÓNICO.

Se entiende como documento íntegro a aquel que contiene toda la información que constaba al momento de su emisión, y que desde entonces no ha sido alterado[42]. La legislación francesa fue una de las primeras que requirió de este elemento para que el documento pudiera ser considerado como prueba. Cuando se analizó los principios de la Ley de Comercio Electrónico, se

---

1. *La documentación del programa, las descripciones de los ficheros y las instrucciones de los programas deben ser elegibles directamente, y deben estar cuidadosamente puestos al día bajo la responsabilidad de la persona que tiene la custodia.*
2. *El documento definido en el apartado uno anteriormente mencionado, deben ser conservados de una forma comunicable tanto tiempo como las grabaciones a las que ser refieren.*

*Si por cualquier razón, los datos grabados son trasferidos de un soporte informático a otro, la persona responsable debe demostrar la concordancia.*

[42] RIOFRÍO Juan Carlos, "La Prueba Electrónica" Editorial TEMIS S. A. Bogotá Colombia, 2004, pág. 105

destacó el Art. 7, el cual dispone que un mensaje de datos permanece íntegro si mantiene completo e inalterable su contenido, salvo algún cambio de forma, propio del proceso de comunicación, archivo o presentación. A su vez el Art. 6 del Reglamento a la Ley de Comercio Electrónico, manifiesta que este requisito se cumple si el mensaje de datos está firmado electrónicamente.

Este principio se deriva de que los documentos electrónicos, así como la firma digital y el mensaje de datos, sean fielmente reproducidos en los sistemas ópticos y su contenido sea el mismo que los documentos originales[43].

Al tenor de este principio surge la exigencia que el almacenamiento de documentos, sea sin edición alguna en forma íntegra y con fidelidad, igual que el documento original y manteniendo el orden consecutivo en el que se creó[44].

Es en atención a este principio de integridad que se asigna la carga de la prueba a la parte que mantenga que los datos han sido alterados, demostrándose la insuficiencia del procedimiento de seguridad empleado[45].

Así, pues, los documentos electrónicos gozan de la presunción de que los datos no han sido alterados, garantizándose que los elementos contractuales son válidos, hasta que se demuestre lo contrario, por vía de los fallos en los procesos de seguridad, o bien por la manifiesta alteración de los documentos electrónicos al ser cotejados con los originales si existiere con copia de respaldo, por la parte que los refuta de falso[46].

---

[43] DELEON Batista, Hernán, "Fuerza Probatoria De Los Documentos Electrónicos", **AR: Revista de Derecho Informático,** ISSN 1681-5726, Edita: Alfa-Redi, http://www.alfa-redi.org/rdi-articulo.shtml?x=1064

[44] DELEON Batista, Hernán, "Fuerza Probatoria De Los Documentos Electrónicos", **AR: Revista de Derecho Informático,** ISSN 1681-5726, Edita: Alfa-Redi, http://www.alfa-redi.org/rdi-articulo.shtml?x=1064

[45] DELEON Batista, Hernán, "Fuerza Probatoria De Los Documentos Electrónicos", **AR: Revista de Derecho Informático,** ISSN 1681-5726, Edita: Alfa-Redi, http://www.alfa-redi.org/rdi-articulo.shtml?x=1064

[46] DELEON Batista, Hernán, "Fuerza Probatoria De Los Documentos Electrónicos", **AR: Revista de Derecho Informático,** ISSN 1681-5726, Edita: Alfa-Redi, http://www.alfa-redi.org/rdi-articulo.shtml?x=1064

## FIRMA ELECTRONICA[47]

La firma electrónica es una forma de identificación que una persona realiza sobre un documento electrónico, para darle autenticidad y demostrar que aprueba su contenido.

"El término firma electrónica es genérico se refiere a las diferentes maneras en que una persona puede indicar una asociación a un documento electrónico. Las firmas digitales son una forma de firma electrónica y tienen las siguientes características: Son únicas para una sola persona, son capaces de ser verificadas, indican si un documento fue alterado después de que fue firmado. Una entidad certificadora es quien otorga la verificación de que una firma efectivamente pertenece a quien dice tenerla. Las firmas digitales son creadas usando un método de encriptación asimétrica, con el cual se crean dos llaves, una pública y otra privada; el método está basado en funciones de algoritmos para generar estas dos llaves diferentes pero muy relacionadas entre sí y las cuales son usadas para encriptar y desencriptar un mensaje.[48]"[1]

**En Ecuador**, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de Datos en su Art. 13 define a la firma electrónica en los siguientes términos: "*Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos*".

La firma electrónica permite:

[47] ENCALADA Ochoa Graciela; "Firma Electrónica y Firma Digital", Tesina previa al Grado de Diplomada en Informática Jurídica. Universidad de Cuenca, diciembre 2008.

●[48] Temas de Derecho Informático. Autores: Gaudencio Delgado Flores y Julio Téllez Valdés. Primera Edición, junio de 2006.

●Garantizar la integridad del mensaje; es decir, que los datos no han sido modificados desde su emisión hasta la recepción de los mismos, por tanto podemos decir que no permite alteración.

●Identificar a las partes firmantes; es decir, a quién ha generado el documento. La firma garantiza que el firmante o los intervinientes son quienes dicen ser.

●La confidencialidad, ya que el contenido, al estar cifrado, solo puede ser conocido por el firmante o por aquellos a quienes el firmante autorice el acceso al documento.

●El no repudio entre las partes. Esto es, se garantiza que el firmante o las partes firmantes son quienes dicen ser, por tanto ninguno de ellos puede negar haber firmado, enviado o recibido el documento.

●La firma electrónica en nuestro país tendrá igual validez y efectos jurídicos que una firma manuscrita en relación con los datos constantes en los documentos y será admitida como prueba en juicio.

***Elementos que intervienen en una firma electrónica.***

**SIGNATARIO O EMISOR**: Es la persona física que actúa en nombre propio o en el de una persona natural o jurídica a la que representa. El signatario firma el documento mediante:

- ●Dispositivo de creación de firma, que consiste en una aplicación o programa informático software que aplica los datos de creación de firma (clave privada) al texto que se pretender firmar y que posee el signatario.
- ●Datos de creación de firma, que son códigos o claves criptográficas privadas que el signatario utiliza para crear la firma electrónica.

**RECEPTOR**:

- Datos de verificación de firma.- Son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica. Se trata de una clave pública utilizada para desencriptar el mensaje.
- Dispositivo de verificación de firma.- Al igual que el dispositivo de creación de firma, el de verificación es otro programa o aplicación informática (software) que aplica los datos de verificación de firma o clave pública y que debe detectar cualquier alteración o modificación de los datos firmados.

**Funcionamiento de la firma electrónica.**

- El emisor elabora un texto, para evitar que sea muy extenso, utiliza el dispositivo de creación de firma y aplica sobre el texto la función “hash”, que es el algoritmo matemático que comprime el mensaje, obteniendo el resumen digital; posteriormente el emisor aplica al resumen su clave privada (Datos de creación de firma), obteniendo de este modo su firma electrónica. El emisor envía el mensaje encriptándolo con la clave pública del receptor o destinatario, el mismo mensaje se firma con la clave privada del emisor.

- Recibe los datos el receptor, coloca su clave privada sobre los datos encriptados y obtiene el texto, la firma electrónica y el certificado digital, y aplicando la clave pública del emisor constata la veracidad de la firma y podrá descifrar el mensaje con su clave privada (es decir la del receptor). Existe un directorio de claves públicas que pueden ser conocidas a través de Internet, este directorio está abierto para todas las personas.

**Obligaciones del titular de la firma electrónica:**

El titular de la firma electrónica tiene ciertas obligaciones, éstas son:

●Tener bajo su estricto control la firma electrónica para evitar la utilización no autorizada.

●Notificar a las personas vinculadas, si existe riesgo de que su firma sea controlada por otras personas no autorizadas.

●Verificar la exactitud de sus declaraciones.

●Responder por las obligaciones que se deriven del uso no autorizado de su firma, cuando no hubiese tomado las medidas necesarias para evitarlo.

●Notificar a la entidad de certificación de información los riesgos sobre su firma y solicitar oportunamente la cancelación de los certificados; y,

●Las demás señaladas en la Ley y sus reglamentos.

**Duración de la firma electrónica.**

La firma electrónica en el Ecuador tendrá duración indefinida, puede ser revocada, anulada o suspendida de conformidad a lo establecido en la Ley 67 y en el reglamento respectivo.

**Extinción de la firma electrónica.**

La firma electrónica se extinguirá por las siguientes circunstancias:

●Por voluntad de su titular

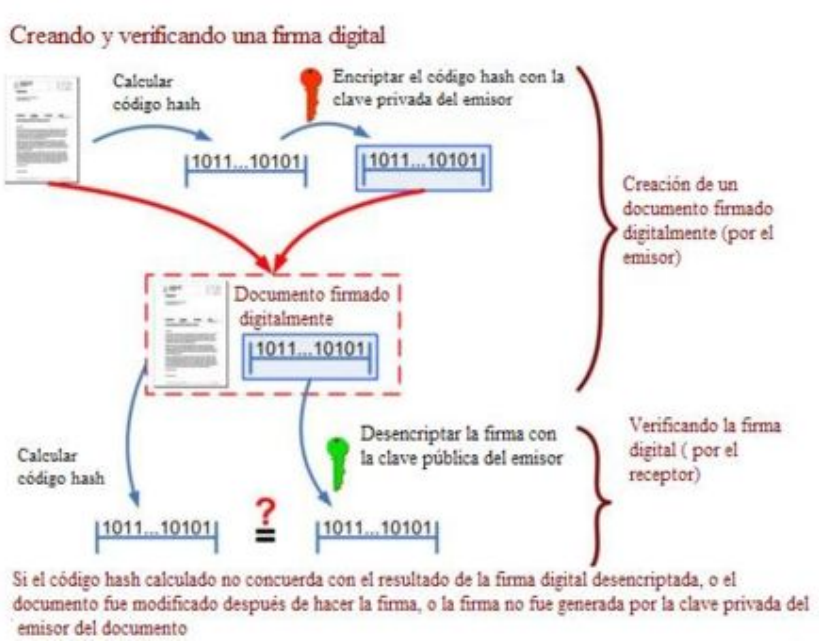
●Por fallecimiento o incapacidad del titular

●Por disolución o liquidación de la persona jurídica, titular de la firma; y,

●Por causa judicialmente declarada.

Según nuestra Ley de Comercio Electrónico, la extinción de la firma electrónica no exime a su titular de las obligaciones previamente contraídas derivadas de su uso.

## FIRMA DIGITAL




La firma digital de un documento es el resultado de aplicar cierto algoritmo matemático, denominado función hash, a su contenido, y seguidamente aplicar el algoritmo de firma (en el que se emplea una clave privada) al resultado de la operación anterior, generando la firma electrónica o digital.

La función **hash** es un algoritmo matemático que permite calcular un valor resumen de los datos a ser firmados digitalmente, funciona en una sola dirección, es decir, no es posible a partir del valor resumen calcular los datos originales. Cuando la entrada es un documento, el resultado de la función es un número que identifica casi inequívocamente al texto. Si se adjunta este número al texto, el destinatario puede aplicar de nuevo la función y comprobar su resultado con el que ha recibido. No obstante esto presenta algunas dificultades por el usuario, para ello se usan software que automatizan tanto la función de calcular el valor hash como su verificación posterior.

## DIFERENCIAS ENTRE FIRMA ELECTRÓNICA Y FIRMA DIGITAL

"La firma electrónica es cualquier método o símbolo basado en medios electrónicos, utilizado o adoptado por una parte con la intención actual de vincularse o autenticar un documento, cumpliendo todas o algunas de las funciones características de una firma manuscrita.

La firma digital es una forma específica de firma electrónica en la cual interviene un proceso criptográfico que da seguridad a quien extiende dicha firma".[49]

La firma digitalizada es una copia electrónica de la firma, es decir, se trata de un simple gráfico en formato digital (puede ser en formato de imagen GIF, JPG, etc.) que la reproduce.

La firma digitalizada se puede obtener al "escanear" un papel en el que conste la firma manuscrita de la persona.

LA EFICACIA PROBATORIA DE LOS DOCUMENTOS ELECTRONICOS SIN FIRMA

Se ha fortalecido la eficacia natural de los documentos electrónicos debidamente firmados, permitiendo que entren por la puerta ancha del proceso, con presunciones de validez y autenticidad. Pero si el documento no está firmado «*siempre estará al margen de su consideración documental, y por ende podrá entrar, pero solamente por la estrecha ventana pericial*[50]*.*

[49] Fernández Delpech, Horario "Internet: Su Problemática Jurídica". ABELEDO-PERROT. Página 255.

[50] RIOFRÍO Martínez-Villalba, Juan Carlos "Eficacia Natural Probatoria de los Documentos Electrónicos No Firmados" No. 062 - Septiembre del 2003, AR: Revista **de Derecho Informático,** ISSN 1681-5726, Edita: Alfa-Red, http://www.alfa-redi.org/rdi-articulo.shtml?x=1288

El valor probatorio de los documentos en general, se han visto siempre sometido a consideraciones legales, por ejemplo se ha establecido supuestos, como el valor que se da a una letra de cambio suscrita, como a un documento cualquiera que reconoce una deuda pero no esta firmado; en este caso el valor probatorio ha sido determinado por reglas normativas pero también se ha suplido vacíos con la jurisprudencia.

En el caso del documento electrónico se aplica el principio equivalencia funcional, *"en otras palabras, cuando la ley requiera ad substantiam, ad probationem o ad solemnitatem que un acto jurídico determinado deba realizarse por escrito, este requisito se considerará cumplido cuando la información conste en forma de mensaje de datos."*[51]

*La mayor parte de las pruebas electrónicas carecen de firmas y certificado, entonces «cuando la Ley no determine el valor de un medio probatorio, entonces el Juez tiene la mayor libertad, pudiendo atribuir a aquel medio el valor de una prueba plena, o negarle también el de simple indicio». Pese a esta verdad teórica, en la práctica algunos jueces temen aceptar como prueba algo no regulado por la ley, creyendo muchas veces de modo timorato e infundamentado que prevaricarían si la admitieran. Así terminan escapando a sus ojos medios por los cuales podrían llegar a la certeza de un hecho, o por lo menos, a un mejor conocimiento… Se puede afirmar que el documento electrónico podría constituir principio de prueba por escrito en el sentido del art. 2724, C.C. En efecto, como ha afirmado muchas veces la jurisprudencia, no es necesario que el principio de prueba escrita esté suscrito por aquellos contra quienes se exige la prueba testimonial, ni que la suscripción sea reconocida*». Pero además, como se verá, un documento electrónico eventualmente podría llegar a ser más que un mero principio de prueba[52].

Sin embargo, en el proceso penal si el documento aunque carente de firma y certificado electrónico, es necesario se examine si coincide con los

[51] RIOFRÍO Martínez-Villalba, Juan Carlos "Eficacia Natural Probatoria de los Documentos Electrónicos No Firmados" Pág. 4-5
[52] RIOFRÍO Martínez-Villalba, Juan Carlos "Eficacia Natural Probatoria de los Documentos Electrónicos No Firmados" Pág. 6.

testimonios, y la misma prueba pericial, lo que determinará si sufrió cambios en el caso de la integridad y si se trata de autenticidad de los documentos no firmados es necesario comprobar la propiedad, posesión o uso del elemento material que contenga estos documentos, del acusado en el tiempo que coincida con el hecho que se juzga.

## 3.5 LA AUTENTICIDAD DEL DOCUMENTO ELECTRÓNICO.

Se dice que un documento es auténtico cuando es fiel reflejo de la voluntad de sus creadores, siendo más seguro, cuanto más difícil es alterar las declaraciones de voluntad en el contenido.

*Carnelutti define a la autenticidad como la correspondencia entre el autor aparente y el autor real del documento, dependiendo esta de la seguridad con la que se cerró el proceso de elaboración y emisión de un Documento.*

*La falta de autenticidad del documento, puede deberse, en el caso del documento electrónico, a alteraciones en la fase de memorización o, en la fase de elaboración, o en la fase de transmisión.*

Sin embargo, manifiesta Bernard E Amory, que podemos entender la autentificación como la actividad de Internet que muestra la cara al autor de un mensaje y la forma de verificar que dicho autor se obliga a dar fe legalmente con el mismo.

*Luis Maria Gatti, distingue de una forma más precisa la identificación y la autentificación, calificándola de identificación como una operación pasiva que puede tener lugar aun ignorando la persona que la recibe; siendo por el contrario la autentificación el proceso activo por el cual cada interlocutor se identifica conscientemente en cuanto al contenido de lo firmado y se adhiere al mismo, por lo que hay algunos métodos que si bien permite una identificación,*

*no llegan a presumir la autentificación, la intención de obligarse. Es imprescindible para contratar electrónicamente de un proceso óptimo de autentificación, hoy en día existe un sin número de métodos para evitar en la medida de lo posible, esas alteraciones, como puede ser el doble tecleo, particulares programas de control, la verificación del mensaje, la utilización del testing, programas de par y edad y disparidad sobre cada carácter, y posteriormente sobre todo los bytes que contiene la misma posición dentro del caracter trasmitido, controles y registros en la actividad de posibles intervinientes, en la elaboración y transmisión de un determinado mensaje. Podemos clasificar en tres grandes categorías las técnicas de autentificación del documento electrónico:*

- *El código secreto o código de ingreso.*
- *La criptografía.*
- *Técnicas basadas en biometría.*

*El código secreto o código de ingreso, supone una combinación determinada de números o letras que sólo es conocida en principio por el titular del mismo. La doctrina anglosajona lo denomina personal identification number o PIN, combinándose usualmente con la utilización de tarjetas magnéticas.*

*La criptografía es un sistema de codificación de un texto o comunas claves confidenciales y de procesos matemáticos complejos (algoritmos) de forma que resulte incomprensible para el tercero que desconozca la clave decodificadora; entendiendo por descodificación la actualización que restablece el texto en un formato original. DELPESO, de una forma más sencilla y concisa define la criptografía "como el arte de hacer incomprensible a todos un mensaje a no ser que conozca la clave secreta."*

*Métodos basados en la biometría, podemos entender la identificación de un determinado operador a través de datos físicos o biológicos, si bien en este caso necesitaríamos un sistema auxiliar para verificar la autenticidad del contenido del documento.*

*Pero a pesar de todas estas medidas de control y otras muchas existentes para garantizar la autenticidad del documento informático, no se lo puede hacer de forma absoluta ya que un tercero pudo intervenir la transmisión. Sin embargo tiene las mismas inseguridad que un documento de puño y letra.*

*Las técnicas de autentificación y su fiabilidad determinan la fuerza probatoria del documento electrónico, vinculando las partes a la inalterabilidad el documento y a la seguridad técnica y operativa del sistema.*

La comisión de las Naciones Unidas para el derecho comercial internacional en el año de 1985 emitió recomendaciones, en las que propugna la autenticación de los documentos electrónicos.

*Uno de los aspectos que disminuye el valor y la confiabilidad de los documentos electrónicos es la ausencia de firmas, las cuales son caracteres que identifican al signatario y sea un instrumento que exprese la voluntad de las partes.*[53]

En nuestro país se aceptan las firmas electrónicas, las cuales se están emitiendo por el Banco Central del Ecuador, ya que esta es una entidad de certificación actualmente en funcionamiento y que puede garantizar la autentificación del documento, ya que en los certificados emitidos se establecen los datos de la persona, garantizándose el saber que es su titular así como también su integridad.

## CERTIFICADOS DE FIRMA ELECTRÓNICA

La Ley 67, define lo que es un certificado de firma electrónica en los siguientes términos: “Es el mensaje de datos que certifica la vinculación de una firma electrónica con una persona determinada, a través de un proceso de comprobación que confirma su identidad”; este documento se utilizará para

[53] CARRARA López, Valentín, “Valor Probatorio del Documentos Electrónico” UNED Centro Regional de Extremadura, MERIDA1995 pág. 165 hasta 167.

certificar la identidad del titular de firma electrónica, para ser considerado válido un certificado de firma electrónica, debe cumplir con ciertos requisitos:

●Identidad y domicilio de la Entidad de Certificación.
●Los datos del titular del certificado para su identificación y ubicación.
●El método de verificación de la firma del titular del certificado.
●Fechas de emisión y expiración del certificado.
●Número único de serie que identifica el certificado.
●La firma electrónica de la entidad de certificación de información.
●Las limitaciones o restricciones para los usos del certificado;
●Y las demás que se establecieren en la Ley de Comercio Electrónica y el Reglamento respectivo.

El plazo de validez de los certificados de firma electrónica, salvo acuerdo contractual, es el dos años a partir de su expedición; cuando se trata de certificados de firma electrónica emitidos con relación al ejercicio de cargos públicos o privados, la duración del certificado de la firma electrónica podrá ser superior a los dos años pero no podrá exceder el tiempo de duración de dicho cargo a menos que exista una de las prórrogas de funciones establecidas en la ley.

Extinción de los certificados de firma electrónica:

●A solicitud del titular
●Por extinción de la firma electrónica
●Por expiración del plazo de validez del certificado de firma electrónica.

La extinción opera desde el momento de su comunicación a la entidad de certificación, excepto en el caso de fallecimiento del titular, en este caso se extingue desde el momento del fallecimiento. Si se trata de personas secuestradas o desaparecidas, los certificados de firma electrónica se extinguen desde el momento de su denuncia ante las autoridades competentes, la extinción del certificado no libera al titular de las obligaciones previamente contraídas, respecto de su uso;

SUSPENSIÓN TEMPORAL

Las causas son las siguientes:

●Cuando el Consejo Nacional de Telecomunicaciones así lo disponga, por causas previstas en la ley.

●Cuando haya falsedad comprobada por parte de la entidad certificadora, de los datos proporcionados por el titular.

●Por incumplimiento del contrato celebrado entre las partes.

Esta suspensión tiene que ser notificada al titular del certificado y al organismo de control, señalando las causas que motivaron la suspensión, una vez que desaparezcan las causales de suspensión o por resolución del Consejo Nacional de Telecomunicaciones, se les habilitará de inmediato el certificado de firma electrónica.[54]

## 3.6 LA REPRODUCCIÓN DEL DOCUMENTO ELECTRÓNICO.

Este principio de la prueba electrónico es elemental; sin embargo, resulta sumamente importante debido a que el documento electrónico debe conservar la información en él contenida. No puede ser volátil, un ejemplo de esto sería los chats, en donde se escribe e interactúan dos o más personas; sin embargo, algunos mensajes no son posibles guardar, y una vez cerrados ya no es posible su recuperación.

Por esta razón es importante demostrar al Tribunal para que se cercioren que la prueba electrónica actuada en el juicio, cumple con este

[54] ENCALADA Ochoa, Graciela, FIRMAS ELECTRÓNICAS Y FIRMAS DIGITALES, tesina previa a la obtención del Grado de Diplomada Superior en Informática Jurídica. 2008

requisito, siendo importante que contemos con los equipos técnicos para la demostración por parte del perito que analizó los otros dos requisitos.

## CONCLUSIONES.

El análisis de la prueba electrónica y principalmente de la documental, no es del todo diferente al del documento tradicional, lo que sucede, es necesario poner mucho énfasis en tratar de determinar elementos que permitan concebir a un documento como inalterado y válido, capaz de sustentar presunciones que lleven a determinar la existencia del delito y sus responsables.

Sin embargo, la prueba documental requiere un examen y cuidado mucho mayor que los documentos tradicionales, ya que pueden desaparecer o modificarse más fácilmente que otros tipos de prueba material. Por ello es necesaria la intervención de peritos que conozcan sobre informática forense para que traten de encontrar las huellas que determinen una información importante en la investigación penal.

Pero no solamente es importante un buen profesional, sino que las técnicas de investigación sobre este tipo de evidencias empleadas por fiscales y policías judiciales sean escrupulosas, con el objeto de garantizar que el documento no sufra alteraciones o deje de tener validez por errores legales en su acopio, ya que puede afectarse la constitucionalidad y validez de la prueba, si se actúa sin autorizaciones del Juez de Garantías Penales por afectar el secreto de las comunicaciones, correspondencia virtual, datos personales, etc. Incluso el análisis más inocente en un celular de las llamadas efectuadas, puede poner en juego el resultado de toda la investigación, como el caso del Sr. Jorge Hugo Reyes Torres, que por medio del recurso de revisión consiguió su libertad, en razón de que la policía había revisado la llamadas efectuadas y mensajes de celular a algunos miembros de la familia, sin autorización de ningún tipo.

Establecer diferencias entre los distintos tipos de documentos electrónicos para darle mayor validez a unos y a otros no, resulta un asunto secundario, ya que el documento público o privado tendrá un peso semejante si se demuestra su autenticidad, integridad y reproducción. También resulta inocuo discutir sobre el valor de un original y una copia en este tipo de soporte, ya que la valoración distinta se producía si la copia puede variar del original; sin embargo, al ser las copias tan exactas como su original y si se demuestra su integridad con elementos como firmas electrónicas o digitales, no merece una valoración inferior a la primera.

Ahora bien, los principios rectores del documento electrónico, en el campo del Comercio, y dispuestos en la Ley de Comercio Electrónico, lo que buscan es su reconocimiento y no discriminación por el soporte utilizado y su equidad al documento en papel, principios que resultan interesantes al rato de sopesar su valor probatorio y formar criterio.

La integridad, por ejemplo es importante sea demostrada, ya que este tipo de documentos pueden ser alterados con mayor facilidad y sin que a simple vista se note. Sin embargo, los sistemas informáticos permiten descubrir estas alteraciones por lo que se vuelve necesario contar con un técnico que sepa y maneje bien las evidencias electrónicas.

Otro aspecto a ser tomado en consideración es la autenticidad del documento electrónico, que permite vincular a alguna persona su autoría, esto debido a que la utilización de las TIC´S permiten el anonimato, lo que vuelve difícil determinar la persona o personas que crearon el documento electrónico y/o la persecución del delito. Así mismo un análisis técnico profundo, unido a otros indicios adquiridos en la investigación determinarán su autoría. La ley ha dispuesto que la firma electrónica con los certificados emitidos por las entidades autorizadas, (en nuestro caso por el Banco Central del Ecuador) son aptas para establecer este vínculo, así como para garantizar su integridad.

Pero también es cierto que los documentos que carezcan de estos elementos, no dejan de tener validez, lo que sucede es que debe demostrarse a cabalidad el cumplimiento de los principios de autenticidad, integridad y reproducción por medios técnicos, una vez demostrado esto, deberán ser valorados en la misma medida que los documentos firmados. Por ello es importante no solo un análisis riguroso técnico, sino también el unir a otros indicios la información en ella contenida para que sea creíble, por lo que se deberá relacionar a los testimonios y prueba material.

# BIBLIOGRAFÍA

**a. Doctrinarias:**

## I LIBROS

AGUILAR J, Rodolfo, “La verdad y la Prueba en Materia Penal”, Sin editorial, Loja Ecuador, 1998.

BAYTELMAN A Andrés y Duce J Mauricio, “Litigación Penal Juicio Oral y Prueba” Colección Derecho Editorial Universidad Diego Portales, Santiago de Chile, 2004.

BAYTELMAN A Andrés y Duce J Mauricio, “Litigación Penal y Juicio Oral” Fondo Justicia y sociedad, Fundación Esquel -USAID, sin año

CARRARA López, Valentín, “Valor Probatorio del Documentos Electrónico” UNED Centro Regional de Extremadura, MERIDA,1995.

CARRASCOSA López, Valentín “Valor Probatorio del Documento Electrónico”, Revista Informática y Derecho 8, UNCD Centro Regional de Extremaura, Mérida 1995.

COUTURE, Eduardo, “Valoración Judicial de las Pruebas”, Editorial Jurídica de Colombia, Tercera Edición, Colombia, 2008.

CHIRA Vargas Machuca, Felix Enrique, “Absorción atómica. Como absolver o Condenar en el Debido Proceso” Editorial Jurídica Griley, Lima, 2007.

DELPESO Navarro, Emilio, “Peritaje Informático” Segunda Edición, Revista Editada por Informes Europeos Expertos IEE y Díaz Santos.

POZO Montesdeoca Carlos, “Práctica del Proceso Penal” Segunda Edición, Editorial Abya Ayala, Quito, Ecuador, 2006.

RIOFRÍO Juan Carlos, “La Prueba Electrónica” Editorial TEMIS S. A. Bogotá Colombia, 2004.

SIGÜENZA Bravo Marco, “Apuntes de Derecho Procesal Penal” Editorial SICMA, primera Edición, Cuenca Ecuador, sin año.

VACA Andrade, Ricardo, “Manual de Derecho Procesal Penal” Cuarta Edición, Editorial Corporación de Estudios y Publicaciones, Tomo I y II, Agosto de 2009, Quito Ecuador.

“Nuevo Sistema Procesal Penal, Guía de Aplicación para el Profesional del Derecho”, Publicación del Fondo de Justicia y Sociedad del Fundación ESQUEL, Ecuador 2003

**II PÁGINAS WEB:**

Del PINO, Santiago, “Manual de Evidencias Digitales y Entornos Informáticos”, http://www.fiscalia.gov.ec/images/Documentos/ManualEvidencias.pdf Acceso 12 de octubre del 2009.

Del PINO, Santiago, “Introducción a la Informática Forense”, http://www.fiscalia.gov.ec/images/Documentos/InformaticaForense.pdf Acceso 13 de octubre del 2009.

DELEON Batista, Hernán, “Fuerza Probatoria De Los Documentos Electrónicos”, **AR: Revista de Derecho Informático,** ISSN 1681-5726, Edita: Alfa-Redi, http://www.alfa-redi.org/rdi-articulo.shtml?x=1064

ENCALADA Ochoa, Graciela, FIRMAS ELECTRÓNICAS Y FIRMAS DIGITALES, tesina previa a la obtención del Grado de Diplomada Superior en Informática Jurídica. 2008.

MEDRANO Molina, Josep Manuel "La Práctica de la Prueba por Soportes Informáticos y Audiovisuales en el Proceso Penal" No. 061 - Agosto del 2003, AR: Revista de Derecho Informático, http://www.alfa-redi.org/rdi-articulo.shtml?x=1310

RIOFRÍO Martínez-Villalba, Juan Carlos, "Eficacia Natural Probatoria de los Documentos Electrónicos No Firmados" No. 062 - Septiembre del 2003, AR: Revista de Derecho Informático, ISSN 1681-5726, Edita: Alfa-Red, http://www.alfa-redi.org/rdi-articulo.shtml?x=1288

Manual Básico de Cateo y Aseguramiento de Evidencia Digital, http://www.alfa-redi.org/rdi-articulo.shtml?x=7693

Guía Operativa para Procedimientos Judiciales con secuestro de tecnología Informática, http://www.alfa-redi.org/rdi-articulo.shtml?x=6216

Evidencia Digital En Colombia: Una Reflexión Práctica, http://www.alfa-redi.org/rdi-articulo.shtml?x=9330

A las puertas de una Nueva Especialización: La Informática Forense, http://www.alfa-redi.org/rdi-articulo.shtml?x=1382

Conceptos y retos en la atención de incidentes de seguridad y la evidencia digital, http://www.alfa-redi.org/rdi-articulo.shtml?x=1507

Documento Electrónico, http://www.alfa-redi.org/rdi-articulo.shtml?x=1465

El documento electrónico: algunas vías de aplicación en el Derecho Probatorio Chileno

http://www.alfa-redi.org/rdi-articulo.shtml?x=225

Las Nuevas Tecnologías Aplicadas al Proceso Jurisdiccional y en Particular la Prueba Digital en el Derecho Uruguayo Vigente, http://www.alfa-redi.org/rdi-articulo.shtml?x=8414

Fuerza Probatoria de los documentos electrónicos, http://www.alfa-redi.org/rdi-articulo.shtml?x=1064

**Legislación Nacional,** textos completos obtenidos del sistema LEXIS.

Constitución de la República del Ecuador, R.O. 449 del 20 de octubre del 2008.

Código de Procedimiento Penal, R.O. Suplemento 360 del 13 de enero del 2000.

Reformas al Código de Procedimiento Penal, R.O. Suplemento 555 del martes 24 de marzo del 2009.

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. Ley 67, publicada en el R.O. Suplemento 557, del 17 e abril del 2002.

Reglamento a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, Decreto Ejecutivo 3496,