INFORMATICA

Según lo planteado por Galindo (2010) “Informática se deriva de la unión de dos palabras acuñada en Francia en el años de 1962, INFOrmacion autoMATICA” (Pablos, Lopez, Romo y Medina. 2010, p. 14).

Por otra parte, se le concibe como “La rama de la Ingeniería que estudia el hardware, las redes de datos y el software necesarios para tratar información de forma automática”. (Universidad de Sevilla, 2017).

CIENCIAS FORENSES

De acuerdo con manual de Ciencias Forenses se puede afirmar que las **Ciencias Forenses** “Forman parte de las llamadas disciplinas biológico-sociales, ya que su objetivo trasciende al hombre como individuo para extenderse al contexto social” (Rocañin, Forneiro, Iglesia. 2007. p. 14).

Discovery Communications plantea:

La definición del diccionario de ciencia forense es la aplicación de prácticas científicas dentro del proceso legal. Esencialmente esto se traduce en investigadores altamente especializados o criminalistas, que localizan evidencias que sólo proporcionan prueba concluyente al ser sometidas a pruebas en laboratorios.

Parte de la evidencia que hallan a menudo no puede ser vista a simple vista, a veces es hasta más pequeña. La ciencia forense ahora usa de manera rutinaria ADN en delitos seriamente complejos, solucionando muertes a partir de estos bloques estructurales de la vida.

Mientras los criminales han desarrollado maneras cada vez más ingeniosas de quebrantar la ley, nuestras fuerzas policiales han tenido que idear maneras más efectivas para someterlos a la justicia. Incluso cuando pareciera que un criminal desapareció sin dejar rastro, los detectives se percataron hace ya un buen rato que esto simplemente no es cierto.

Con cada contacto que establecemos con un lugar, objeto o incluso otra persona, se deja una presencia física. Todos sabemos que las huellas dactilares y las fundas de una bala pueden delatar a un ladrón, pero ¿sabías que las fibras, los cabellos extraviados e incluso hasta el sucio de tus zapatos pueden implicarte en una investigación criminal?. De hecho, casi todo lo que se encuentra en la escena de un crimen puede ser sometido a prueba y usado como evidencia para probar o refutar la presencia de un sospechoso. (Discovery Communications. 2017).

INFORMATICA FORENSE

Teniendo en cuenta lo dicho por Zuccardi el concepto de Informática Forense se refiere a:

Según el FBI, la informática (o computación) forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional.

La informática forense hace entonces su aparición como una disciplina auxiliar de la justicia moderna, para enfrentar los desafíos y técnicas de los intrusos informáticos, así como garante de la verdad alrededor de la evidencia digital que se pudiese aportar en un proceso (Zuccardi, G, Gutiérrez, J, 2006, p.

EVIDENCIA DIGITAL

De acuerdo a lo citado en Informática Forense Eurolatinoamerica, la evidencia digital en concebida como:

Cualquier valor probatorio de la información almacenada o transmitida en formato digital de tal manera que una parte o toda puede ser utilizada en el juicio Antes de aceptar la evidencia digital un tribunal determinará si la prueba es pertinente, auténtica, si es un rumor y si es aceptable una copia o el original es requerido. (IForense. (2017).

CLASIFICACION 2

1. **Registros generados por computador:**

"Son aquellos, que como dice su nombre, son generados como efecto de la programación de un computador. Los registros generados por computador son inalterables por una persona. Estos son llamados registros de eventos de seguridad (logs) y sirven como prueba". (Zuccardi, G, Gutiérrez, J, 2006, p. 9).

De acuerdo a lo planteado Zuccardi, Gutiérrez (2006, p.9), La Evidencia Digital se clasifica en:

2. **Registros no generados sino simplemente almacenados por o en computadores:**

"Son aquellos generados por una persona, y que son almacenados en el computador, por ejemplo, un documento. En estos registros es importante lograr demostrar la identidad del generador, y probar hechos o afirmaciones contenidas en la evidencia misma". (Zuccardi, G, Gutiérrez, J, 2006, p. 9).

3. **Registros híbridos que incluyen tanto registros generados por computador como almacenados en los mismos:**

"Los híbridos son aquellos que combinan afirmaciones humanas y logs. Para que estos registros sirvan como prueba deben cumplir los dos requisitos anteriores". (Zuccardi, G, Gutiérrez, J, 2006, p. 9).

CRITERIOS DE ADMISIBILIDAD

Según lo contemplado "Legislaciones modernas existen cuatro criterios en cuenta para analizar al momento de decidir sobre la admisibilidad de la evidencia: la autenticidad, la confiabilidad, la completitud o suficiencia, y el apego y respeto por las leyes y reglas del poder judicial" (Zuccardi, G, Gutiérrez, J, 2006, p. 9).

Autenticidad:

Una evidencia digital será auténtica siempre y cuando se cumplan dos elementos:

- Primero: Demostrar que dicha evidencia ha sido generada y registrada en el lugar de los hechos.

- Segundo: Mostrar que los medios originales no han sido modificados; es decir, que los registros corresponden efectivamente a la realidad y que son un fiel reflejo de la misma. (Zuccardi, G, Gutiérrez, J, 2006, p. 9).

De acuerdo a lo definido por Zuccardi se puede establecer que:

Confiabilidad:

Se dice que los registros de eventos de seguridad son confiables si provienen de fuentes que son **creíbles y verificables.** Para probar esto, se debe contar con una arquitectura de computación en correcto funcionamiento que demuestre, que los logs que genera, tienen una forma confiable de ser identificados, recolectados, almacenados y verificados. Una prueba digital es confiable si el "sistema que lo produjo no ha sido violado y estaba en correcto funcionamiento al momento de recibir, almacenar o generar la prueba". (Zuccardi, G, Gutiérrez, J, 2006, p. 9).

De acuerdo a lo definido por Zuccardi se puede establecer que:

Suficiencia o Completitud de las Pruebas:

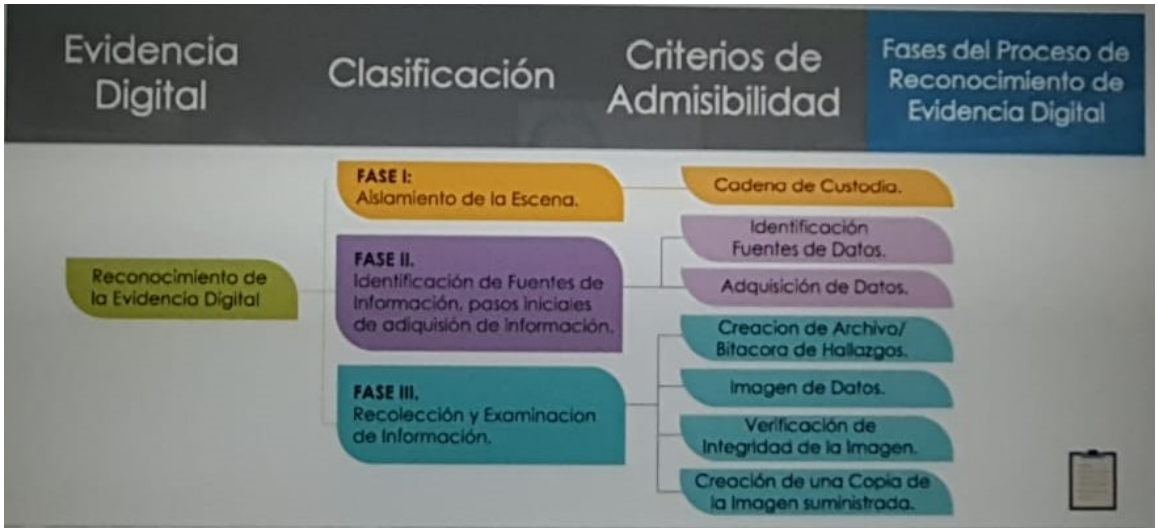
Para que una prueba esté considerada dentro del criterio de la suficiencia debe estar completa. Para asegurar esto es necesario "contar con mecanismos que proporcionen integridad, sincronización y centralización" para lograr tener una vista completa de la situación. Para lograr lo anterior es necesario hacer una verdadera correlación de eventos, la cual puede ser manual o sistematizada. (Zuccardi, G, Gutiérrez, J, 2006, p. 9).

De acuerdo a lo definido por Zuccardi se puede establecer que:

Respeto por las leyes y reglas del poder judicial:

Este criterio se refiere a que la evidencia digital debe cumplir con los códigos de procedimientos y disposiciones legales del ordenamiento del país. Es decir, debe respetar y cumplir las normas legales vigentes en el sistema jurídico. (Zuccardi, G, Gutiérrez, J, 2006, p. 9).

FASES DEL PROCESO DE RECONOCIMIENTO DE EVIDENCIA DIGITAL



EVIDENCIA TRADICIONAL

La evidencia tradicional permite probar y establecer un origen, es difícil de alterar este tipo de evidencia sin que queden rastros de la acción realizada, **es decir que la evidencia tradicional se puede determinar como la evidencia en papel o documentos** que permiten en el caso del papel una lectura directa sin necesidad de equipos especiales o de alta tecnología, la evidencia Tradicional es importante dado que contiene un formato comprensible y asequible a la lectura directa, este tipo de elementos son tratados de acuerdo a las normas de archivo de cada país.
(Valencia, F, Tamayo, J. 2012. p. 99).

EVIDENCIA DIGITAL

Casey define la evidencia de digital como “cualquier dato que puede establecer que un crimen se ha ejecutado (commit) o puede proporcionar una enlace (link) entre un crimen y su víctima o un crimen y su autor**(Casey04).**

“Cualquier información, que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático” **(HBIT03).**

A diferencia de la documentación en papel, la evidencia computacional es frágil y una copia de un documento almacenado en un archivo es idéntica al original. Otro aspecto único de la evidencia computacional es el potencial de realizar copias no autorizadas de archivos, sin dejar rastro de que se realizó una copia **(ComEvi02).**

Esta situación crea problemas concernientes a la investigación del robo de secretos comerciales, como listas de clientes, material de investigación, archivos de diseño asistidos por computador, fórmulas y software propietario.

Debe tenerse en cuenta que los datos digitales adquiridos de copias no se deben alterar de los originales del disco, porque esto invalidaría la evidencia; por esto los investigadores deben revisar con frecuencia que sus copias sean exactas a las del disco del sospechoso, para esto se utilizan varias tecnologías, como por ejemplo checksums o hash MD5 **(DaVa01)**.
(Valencia, F, Tamayo, J. 2012. p. 99).