CONCEPTO DE AUDITORIA FORENSE

Como bien lo define Kata Y. (2013), “La auditoría forense consiste en una evidencia digital que se obtiene por el uso de técnicas de investigación criminalísticas integradas con la contabilidad, conocimientos jurídicos procesales y con habilidades en finanzas de negocios para recabar y manifestar información y opiniones como pruebas ante los tribunales, el análisis resultante además de poder usarse en los tribunales puede servir en disputas de diversa índole”. Se trata de una especialidad relativamente nueva, que demanda alta calificación en conocimientos de informática, y la doctrina del derecho penal y derecho civil.

Para mayor profundidad sobre definiciones como *digital forensics* (forencia digital), y *network forensics* (forencia en redes) recomendamos la publicación de Cano, J., en el acápite definiciones.

## El cómputo forense.

El **cómputo forense**, también llamado **informática forense**, **computación forense**, **análisis forense digital** o **examen forense digital** es la aplicación de técnicas científicas y analíticas especializadas a infraestructuras tecnológicas que permiten identificar, preservar, analizar y presentar datos válidos dentro de un proceso legal.

Dichas técnicas incluyen reconstruir elementos informáticos, examinar datos residuales, autenticar datos y explicar las características técnicas del uso de datos y bienes informáticos.

Como la definición anterior lo indica, esta disciplina no solo hace uso de tecnologías de punta para mantener la integridad de los datos y del procesamiento de los mismos; sino que también requiere de una especialización y conocimientos avanzados en materia de informática y sistemas para poder detectar qué ha sucedido dentro de cualquier dispositivo electrónico. La formación del informático forense abarca no solo el conocimiento del *software* sino también de *hardware*, redes, seguridad, piratería*,* craqueo y recuperación de información.

La informática forense ayuda a detectar pistas sobre ataques informáticos, robo de información, conversaciones o evidencias en correos electrónicos y chats.

La evidencia digital o electrónica es sumamente frágil, de ahí la importancia de mantener su integridad. El simple hecho de pulsar dos veces en un archivo modificaría la última fecha de acceso del mismo.

## La importancia de la Auditoria Forense

La importancia de la Auditoria Forense Informática radica en la necesidad de conocer los mecanismos y herramientas técnico-legales, que permita enfrentar de forma adecuada la creciente y descontrolada ola de criminalidad en nuestro país y en el mundo entero. El caso particular de nuestro país, que vive un periodo de crisis moral profunda en todos los estamentos del estado, es poco lo que se ha avanzado a juzgar por los casos de escándalo que no solo abarca los constantes archivamientos de casos de personajes políticos, como Keiko Fujimori, Alan García, Ollanta Humala, y podríamos sospechar sin mayor esfuerzo, es lo que busca Alejandro Toledo, solo por citar los casos más sonados en torno a los casos Lava Jato, Odebrech, Ecoteva y OAS.

Es increíble que en pleno siglo XXI, que tanto desarrollo ha traído a nivel informático en los diferentes sectores de la economía, en nuestro país no hayamos ido a la par con este desarrollo en la lucha contra el crimen informático organizado.

De modo que hace mucha falta desarrollo de esta profesión técnico legal, con todo el apoyo del sector público, privado y ONGs interesadas en sacar adelante a nuestro país en la lucha contra la corrupción de más alto nivel. Este estudio pretende dar algunos alcances a los interesados en conocer con alguna profundidad la problemática que subyace a la auditoría forense informática.

## TÉCNICAS PARA IDENTIFICAR DELITOS

**TÉCNICAS PARA IDENTIFICAR DELITOS**

* Indagación
* Encuestas
* Inspección
* Comparaciones
* Observaciones

**DIAGNÓSTICO DEL PROBLEMA**

Similar a cuando alguien contrae un mal, el enfermo acude a un médico y luego de ser revisado por el médico y sometido a una serie de preguntas, el médico emite un diagnóstico el cual se nutre de información confiable para no cometer errores. Del mismo modo el profesional forense, debe utilizar información confiable utilizando herramientas confiables y eficaces para tal propósito. Parte del proceso del diagnóstico será la revisión cuidadosa del sistema operativo de la entidad investigada, software de oficina, navegación por internet, etc. El problema puede involucrar la ausencia de un antivirus potente y confiable.

**FORMA DE RECABAR INFORMACIÓN**

Entre los programas más utilizados para conseguir información, se encuentran el FOCA, y el BELARC. El primero de ellos se utiliza para encontrar metadatos (información oculta en documentos) mientras que el segundo construye un perfil detallado del software y hardware instalados en la PC, Kata Y. (2013). Existen otros programas de uso común, como lo son: ENCASE, FORENSIC TOOLKIT, y WINHEX.

**RECONOCIMIENTO DE LA EVIDENCIA DIGITAL COMO EVIDENCIA FORMAL Y VALIDA**



La evidencia digital en la administración de justicia en muchas partes del mundo continúa siendo una situación problemática  por resolver Brungs, A y Jamieson , R. (2003). Es necesario alcanzar la mejor preparación de profesionales con las mejores herramientas disponibles, y dotar de los recursos necesarios para alcanzar este objetivo. Se dice por ejemplo que un audio con declaraciones de un personaje político o tal vez un empresario, que revela un acto delictivo, no sería suficiente para iniciar una demanda de tipo penal, ya que solo es considerado un indicio. En cierto modo esto tiene un cierto asidero, debido a que existe la posibilidad de que la voz no sea la del personaje imputado. Esto obliga a los expertos en tecnología auditiva a desarrollar mecanismos tecnológicos avanzados que certifiquen la autenticidad de este tipo de prueba. En el caso del material inculpatorio encontrado recientemente este año 2017, contra el expresidente Alan Garcia, por ejemplo, las iniciales A.G. encontradas en la agenda de Marcelo Odebrecht, no habría sido prueba categórica para configurar una demanda contra el expresidente. También se sabe que Odebrecht, opera con un software diseñado para almacenar información de los pagos efectuados a personajes políticos, el cual trabaja con seudónimos. Cabe la pregunta: ¿si se demuestra en la información que remitió la autoridad judicial de Brasil, a la autoridad judicial en Perú relacionado con el caso Odebrecht, y se vincula a las cuentas bancarias a las cuales se hizo los depósitos, estaríamos frente a una evidencia irrefutable? Aunque esto suena muy evidente, hay que tener en cuenta que es común que estos personajes trabajan con testaferros de su entera confianza, a los cuales defienden y controlan celosamente.

**ACCIÓN QUE SIGUE AL DIAGNOSTICO**

Luego de reunir toda la información, en forma de evidencia en torno al diagnóstico referido al manejo del software, es recomendable solucionar en 3 fases:

Fase 1:

Adquirir un buen antivirus con licencia, que pueda garantizar la protección de la información de la entidad. Los antivirus piratas no ofrecen ninguna garantía de protección. En el mercado existen muchos antivirus confiables, entre ellos estan el Norton, Avast, Panda, y NOD32, etc.

Fase 2:

En cuanto al sistema operativo, es recomendable Enterprise Agreement, que es un programa completo de licencias por volumen de Microsoft dirigido a grandes corporaciones que manejan más de 250 PC y tienen un departamento de compras centralizado. Ellos normalmente, están siempre interesados en una adecuada protección de su información, y están dispuestos a pagar un alto precio por su seguridad informática.

Fase 3:

Adquisición de las licencias de información geográfica que se utiliza en la empresa (GIS).

Otros:

Es necesario establecer:

Políticas de seguridad

Acuerdos de confidencialidad

Gestión de archivos: Inventario, responsabilidad.

Seguridad de los recursos humanos: Antes, durante y después de empleo

Seguridad física y ambiental: Áreas seguras, protección del equipo.

Gestión de las comunicaciones y operaciones: Protección contra malware, back-up, seguridad de redes, intercambio de información.

Control de acceso: Control de usuarios y privilegios, contraseñas, acceso a redes, control de sistema operativo computación móvil.

Desarrollo y mantenimiento de los sistemas de información: Software desarrollado.

Gestión de incidentes: Control de eventos, Gestión de la continuidad comercial: Respuesta a fallos o desastres críticos. Cumplimiento: Leyes y regulaciones, propiedad intelectual, etc.

**NORMAS INTERNACIONALMENTE RECONOCIDAS**

En respuesta a la imperativa necesidad de mejorar los procedimientos relacionados con la seguridad informática, buscando proteger la información privada y/o del Estado y mejor preservarlo de manejos indeseados, es que conforme fue evolucionando la tecnología, de forma paralela se fueron creando marcos normativos que den adecuado soporte a las nuevas exigencias, sin que esto signifique que esto es un tema concluido.

Entre los distintos organismos relacionados comercial y/o institucionalmente con los temas de Seguridad de la Información, podemos citar los siguientes:

* Normas de Auditoría Generalmente Aceptadas : NAGA
* ISACA: [COBIT](https://plataformavirtual.itla.edu.do/mod/resource/view.php?id=17594)
* British Standards Institute: BSI
* International Standards Organization: Normas ISO
* Departamento de Defensa de USA: Orange Book / Common Criteria
* ITSEC – Information Technology Security Evaluation Criteria: White Book
* Sarbanes Oxley Act, HIPAA
* COSO Report

NORMA ISO 17799:2000

Es una norma con carácter de estándar en el ámbito de la seguridad informática, y está basada en la norma BS 7799, la cual propone 10 áreas de dominio de control consideradas “exitosas” que toda organización debe establecer y cumplir:

* Política de Seguridad de la Información
* Organización de la Seguridad
* Clasificación de los activos
* Seguridad del Personal
* Seguridad Física y Ambiental
* Gestión de Comunicaciones y Operaciones
* Control de Accesos
* Desarrollo y Mantenimiento de Sistemas  
  Administración de la Continuidad de los Negocios
* Villacis, V.  (2006)

NORMAS RELATIVAS A LA EJECUCIÓN DE LA AUDITORIA INFORMÁTICA

De acuerdo a lo señalado por Villacis, V.  (2006), “Para realizar el trabajo de auditoria, debe estar formalmente acreditado ante el respectivo organismo, entidad o dependencia.

Podrán incorporarse al equipo de auditoría, en calidad de apoyo, los profesionales y/o especialistas cuyos conocimientos y experiencia se consideren necesarios para el trabajo que se desarrolla.

Según el alcance de la auditoría, se deberá evaluar el control interno del organismo, entidad, dependencia o área objeto de la misma para determinar su grado de confiabilidad e identificar los aspectos críticos que requieran examen exhaustivo y como consecuencia de ello, establecer la naturaleza, oportunidad, métodos, procedimientos y técnicas aplicables en sus fases anteriores…”

Hasta este punto, como se puede observar, este procedimiento tiene muchas similitudes con los procedimientos de una auditoria operativa. Para mayor profundidad en esta área pueden acudir a la fuente citada en el primer párrafo de éste acápite, en nuestras referencias bibliográficas.

Qué es la pérdida de datos

La pérdida de datos es un incidente que ocurre en los sistemas de información cuyo resultado es que la información se pierde o es destruida por fallos en el almacenamiento, la transmisión o el procesamiento. Los sistemas de información deben implementar equipos y procesos para prevenir la pérdida de datos o restaurar los datos perdidos.

La pérdida de datos (data loss) es diferente de la indisponibilidad de datos (data unavailability), que puede surgir por ejemplo de una interrupción de la red. Aunque ambos tienen consecuencias básicamente similares para los usuarios, la indisponibilidad de datos es temporal, mientras que la pérdida de datos puede ser permanente. La pérdida de datos también es distinta de la violación de la seguridad de los datos (data leak), un incidente donde los datos caen en manos equivocadas o son utilizados por una persona que no está autorizada a hacerlo.

La pérdida de datos puede ser de carácter temporal o permanente. Las pérdidas de datos temporales se caracterizan porque el incidente puede ser remediado, mientras que en una pérdida permanente de datos, los datos no se pueden recuperar, ya que se pierden sin posibilidad de recuperación o son destruidos físicamente.

Respecto a los tipos de pérdida de datos y por qué se produce la pérdida de datos, podemos distinguir entre acciones intencionadas y acciones involuntarias. Dentro de las acciones intencionales podemos citar:

* Eliminación intencional de un archivo o programa.
* Acto malicioso, crimen, como robo, hacking, inyección de SQL, sabotaje, robo de medios físicos.
* Malware, como un gusano o virus.

Como acciones involuntarias que pueden provocar pérdida de datos tenemos las siguientes:

* Inseguridad informática.
* Eliminación accidental de un archivo o programa.
* Errores de administración.
* Incapacidad para leer un formato de archivo desconocido.
* Fallo de alimentación o reinicio (reboot), lo que hace que los datos en la memoria volátil no se guarden en la memoria permanente.
* Error de hardware, como un fallo de disco duro o un crash informático.
* Bloqueo del software, lo que provoca que los datos no se guarden.
* Error de software (bug).
* Mala usabilidad, como no confirmar un comando de eliminación de archivos.
* Fallo del negocio o quiebra del proveedor en el que se almacenan los datos.
* Corrupción de datos, corrupción del sistema de archivos o corrupción de bases de datos.
* Desastres naturales, terremoto, inundación, tornado, etc.
* Fuego, incendio.
* Degradación de datos.

## Qué es el borrado de archivos

El borrado de archivos o eliminación de los mismos, es la acción de eliminar un archivo que se encuentra ocupando un espacio en el disco duro o en un sistema de archivos. Cuando un archivo se elimina, los sectores que este ocupaba en el disco pasan a estar libres y se pueden usar para el almacenamiento de nuevos datos.

Todos los sistemas operativos incluyen comandos para eliminar archivos, tanto en modo consola como en modo gráfico. En modo consola (CLI, Command Line Interface, Interfaz de línea de comandos) existen comandos tales como rm en Linux y Unix, o del/erase en MS-DOS y Windows. En modo gráfico (GUI, Graphical User Interface, Interfaz gráfica de usuario) los administradores de archivos también proporcionan una manera conveniente de eliminar archivos. Puede eliminarse un archivo individual, una selección de archivos o puede borrarse un árbol de directorios completo.

Respecto a los tipos de borrado de archivos, en los sistemas informáticos se pueden identificar dos tipos de borrado de archivos: el borrado común y el borrado seguro.

El **borrado común** es el tipo de borrado habitual, conocido por todos. En este tipo de borrado los archivos no son eliminados por completo. Principalmente lo que sucede es que el disco duro cambia el estado de un grupo de sectores de ocupados a libres, quedando dichos sectores disponibles para almacenar otros archivos. Sin embargo en estos sectores quedan rastros del archivo eliminado que posibilitan la recuperación del archivo.

El **borrado seguro** se hace con la ayuda de una herramienta de software que utiliza algoritmos que permiten la eliminación del archivo sin dejar rastro alguno. Mediante este borrado, los sectores afectados quedan completamente vacíos (a menudo el espacio se llena con ceros y unos aleatorios) y se impide que el archivo pueda ser recuperado en un futuro.

Un problema habitual con los datos sensibles es que los archivos borrados no se borran realmente, sino que la mayoría de los sistemas de archivos sólo eliminan el enlace a los datos, por lo que pueden ser recuperados. Mediante el borrado convencional, los archivos “eliminados” no se eliminan realmente, sino que sólo se marcan como suprimidos, por lo que pueden ser recuperados durante algún tiempo, hasta que los sectores del disco donde se almacenan sean utilizados eventualmente para almacenar otros archivos. Así es como funcionan los programas de recuperación de datos, escaneando archivos que han sido marcados como eliminados.

Qué es un crash informático

**Qué es un crash informático**

El término crash informático (o bloqueo informático) se usa para denominar el hecho de que un programa informático o un sistema operativo, dejen de funcionar de la manera correcta. Este fallo puede ser total o parcial. En ocasiones el programa se “congela” y deja de responder a cualquier acción del usuario o de su entorno, es entonces cuando se habla de crash.

La mayoría de los fallos son el resultado de ejecutar instrucciones de máquina no válidas, tales como utilizar direcciones de memoria incorrectas, desbordamientos de búfer, sobrescribir una parte del código de programa afectado debido a un error anterior, tener acceso a direcciones de memoria no válidas, utilizar un código de operaciones no válido o desencadenar una excepción no controlada. El error de software original que inició esta cadena de eventos suele ser considerado como la causa del bloqueo, que se descubre a través del proceso de depuración. El error original puede estar muy lejos del código que realmente sufrió el bloqueo.

Los crash informáticos pueden tener severas implicaciones de seguridad, ya que muchos errores de software que causan bloqueos también son explotables para la ejecución arbitraria de código y otros tipos de escalada de privilegios. Por ejemplo, un desbordamiento de memoria intermedia puede sobrescribir la dirección de retorno de una subrutina con un valor no válido, lo que causará un error de segmentación. Sin embargo, si un exploit sobrescribe la dirección de retorno con un valor válido, se ejecutará el código en esa dirección. Por ello, un crash informático puede ser producto de una explotación de una vulnerabilidad de forma malintencionada, logrando corromper la integridad del sistema.

Un **crash de aplicación** ocurre cuando un determinado programa pretende realizar una operación prohibida por el sistema operativo, tras lo cual la aplicación se bloquea, el sistema operativo activa una excepción en la aplicación y muestra un cuadro de diálogo con la opción de ejecutar un depurador si está disponible. Algunas aplicaciones intentan recuperarse del error y continuar la ejecución en lugar de salir. Los errores típicos que resultan en bloqueos de aplicación incluyen:

* La aplicación intenta escribir o leer en una ubicación que no le está permitida.
* Intenta acceder a hardware para el cual no tiene permisos de acceso.
* Usa argumentos inválidos para acceder al sistema.
* Intenta acceder a recursos sobre los cuales no se le han otorgado privilegios (error de bus).
* Intenta ejecutar instrucciones de máquina con argumentos erróneos, como división por cero, etc.

Si la aplicación que falla es un software que se ejecuta en un servidor web, el sitio web puede bloquearse, haciéndolo inaccesible por completo o puede mostrar únicamente un mensaje de error en lugar del contenido normal.

Un **crash de sistema operativo**, también conocido como fallo de sistema (en inglés “fatal system error” o “system crash”), se produce cuando un sistema operativo se detiene porque que alcanza una condición en la que ya no puede funcionar con seguridad.

## Qué es un fallo de disco duro

Se habla de un fallo de disco duro cuando éste no responde de forma correcta a sus funciones o no se pueden acceder a la información contenida en él, desde un ordenador correctamente configurado. Un fallo en el disco puede darse durante la operación normal de éste o por causas externas como un fuerte golpe, así como por el contacto con agua, fuego o cualquier otro agente externo que lo afecte en su funcionamiento. Los discos duros también pueden quedar inoperables debido a la corrupción de datos, la destrucción del MBR (Master Boot Record, Registro de arranque maestro) de la unidad de disco duro, o bien a través de malware que destruye deliberadamente el contenido del disco.

La composición de un disco duro hace que también pueda presentar fallos por desgaste de las piezas mecánicas. También existen discos duros con defectos de fábrica, que pueden presentar fallos antes de lo esperado. Generalmente un disco duro que logra trabajar de manera correcta por varios meses, tiene un buen tiempo de vida útil (varios años). Por otra parte, una unidad de disco duro puede fallar en cualquier momento en muchas situaciones diferentes.

La causa más notoria del fallo de la unidad es el “head crash”, que se produce al rozar la cabeza lectora con los discos de almacenamiento de datos magnéticos, causando que uno o más sectores queden defectuosos, lo que generalmente supone una pérdida severa de datos, y los intentos de recuperación de datos pueden causar más daño si no lo hace un especialista con el equipo adecuado.

Respecto a las señales de fallos de disco duro, las fallos en un disco duro pueden ser graduales o repentinos. En un fallo gradual se comienzan a dar señales de pequeñas fallos (problemas en la carga del sistema operativo, un ordenador lento, etc.), que pueden ser reparados o que permiten salvar la información antes de un daño total. En un fallo repentino, por el contrario, se produce una pérdida total del disco de forma inesperado. El fallo gradual de la unidad de disco duro puede ser difícil de diagnosticar, ya que sus síntomas, como datos dañados y la ralentización del PC causados ​​por áreas de fallo gradual del disco duro que requieren repetidos intentos de lectura antes del acceso exitoso, pueden ser causados por muchos otros problemas de la computadora, como el malware.

## Qué es una Copia de seguridad

Una copia de seguridad o backup, es un término que se usa en el ámbito informático para definir las copias que se hacen de un archivo original, con el fin de tener a disposición un punto de recuperación de la información en caso de pérdida por cualquier circunstancia. Con una buena copia de seguridad, se garantiza que información valiosa no se pierda ante cualquier acontecimiento que afecte a los archivos originales.

Las copias de seguridad pueden tener dos propósitos distintos. El propósito principal es usualmente poder recuperar los datos después de su pérdida, ya sea por eliminación o corrupción de datos. El objetivo secundario de las copias de seguridad es poder recuperar los datos históricos de un momento anterior, de acuerdo con la política de retención de datos definida por el usuario. La retención de datos se refiere al almacenamiento de ciertos datos durante un determinado tiempo, generalmente por requisitos legales o reglamentarios.